Calhoun
Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

Theses and Dissertations | Thesis Collection

2005-09

An analysis of automated solutions for the Certification and Accreditation of navy medicine information assets

Gonzales, Dominic V.

Monterey California. Naval Postgraduate School

DUDLEY KNOX LIBRARY

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS OF AUTOMATED SOLUTIONS FOR THE CERTIFICATION AND ACCREDITATION OF NAVY MEDICINE INFORMATION ASSETS

by

Dominic V. Gonzales

September 2005

Thesis Advisor:	Karen Burke
Second Reader:	Douglas E. Brinkley

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE An Analysis of Automated Solutions for the Certification and Accreditation of Navy Medicine Information Assets			**5. FUNDING NUMBERS**
6. AUTHOR(S)			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The purpose of this study was to determine potential improvements in Navy Medicine's current Certification and Accreditation (C&A) process. The study examined whether Navy Medicine's C&A policies are in alignment with DoD, Navy and Federal Government requirements and whether the use of automated C&A tools could significantly improve Navy Medicine's current C&A security posture.

The primary research reviewed C&A policy and included a comparative analysis of two cutting edge automated C&A tools namely, Xacta and eMASS. The findings of the analysis revealed that the use of automated C&A tools could significantly enhance Navy Medicine's C&A process and assist Navy Medicine's information assurance personnel who are responsible for the execution of the Navy Medicine C&A process and approval of Navy Medicine information systems. This study also provided valuable insight in verifying the evidence on how information assurance (IA) controls are addressed within the automated C&A tools regardless of the C&A process. The results of the analysis ultimately led to the development of key recommendations that can assist Navy Medicine in selecting the appropriate automated C&A tool for its C&A process.

14. SUBJECT TERMS certification, accreditation, DITSCAP			**15. NUMBER OF PAGES** 155
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

AN ANALYSIS OF AUTOMATED SOLUTIONS FOR THE CERTIFICATION AND ACCREDITATION OF NAVY MEDICINE INFORMATION ASSETS

Dominic V. Gonzales
Lieutenant, United States Navy
B.S., University of the Philippines, 1986
M.S., Central Michigan University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: Dominic V. Gonzales

Approved by: Karen Burke
Thesis Advisor

Douglas E. Brinkley
Co-Advisor

Dan C. Boger
Chairman
Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this study was to determine potential improvements in Navy Medicine's current Certification and Accreditation (C&A) process. The study examined whether Navy Medicine's C&A policies are in alignment with DoD, Navy and Federal Government requirements and whether the use of automated C&A tools could significantly improve Navy Medicine's current C&A security posture.

The primary research reviewed C&A policy and included a comparative analysis of two cutting edge automated C&A tools namely, Xacta and eMASS. The findings of the analysis revealed that the use of automated C&A tools could significantly enhance Navy Medicine's C&A process and assist Navy Medicine's information assurance personnel who are responsible for the execution of the Navy Medicine C&A process and approval of Navy Medicine information systems. This study also provided valuable insight in verifying the evidence on how information assurance (IA) controls are addressed within the automated C&A tools regardless of the C&A process. The results of the analysis ultimately led to the development of key recommendations that can assist Navy Medicine in selecting the appropriate automated C&A tool for its C&A process.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

C&A	certification and accreditation
DAA	Designated Approval Authority
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
IA	Information Assurance
IATO	Interim Approval To Operate
IS	Information System
ISSO	Information Systems Security Officer
IT	Information Technology
OMB	Office of Management and Budget
RTM	Requirements Traceability Matrix
SFUG	Security Features Users Guide
SRTM	Security Requirements Traceability Matrix
SSAA	System Security Authorization Agreement
ST&E	Security Tests and Evaluation
TFM	Trusted Facilities Manual

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First, I would like to thank God for all His blessings of which I am eternally grateful. Second, I would like to thank the professors and colleagues who shared their time and knowledge in helping me to complete the Information Technology Management curriculum at Naval Postgraduate School. Specifically, I would like to thank Professor Karen Burke for her unwavering dedication, steady guidance, expert advice and endless patience and understanding. I would also like to thank Professor Douglas Brinkley for his invaluable and expedient thesis advisement during the completion of this thesis.

Third, I would like to thank the US Navy, Medical Service Corps, for providing me with the opportunity to further my education in the information technology field. I would like to thank the personnel at SPAWAR San Diego and Charleston, Naval Medical Information Management Command (NMIMC), and Telos Corporation for taking time in providing me with valuable resources in the certification and accreditation process.

Fourth, I am grateful to my parents, Amado and Stella for their endless patience and support. And most importantly, I would like to thank my family who supported and encouraged me in striving to make a better life for them and myself. To my wife Aurora for always being there and my children, Kristin Nicole and Dominic Nicolas, whose unselfish love and understanding truly inspired me and made this thesis possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The U. S. government has gone from a manual method of doing business to a state of information technology (IT) reliance within a relatively few years. Today, the government relies on IT to such a degree that if abruptly taken away, enterprises would crumble. IT comprises much of the critical information infrastructure within the United States.

As technology advances, information systems become more and more complex to keep up with the growing ideas for automation and business benefit of increased productivity and service. The complexity of systems is a driving force for assessing the security using both technical and non-technical approaches. Information security must ensure confidentiality, integrity, and availability to protect the privacy of the public, and at the same time ensure availability of the services that the users of the systems require. It' is a fundamental management responsibility to ensure that the appropriate security controls are in place. Creating a living program to identify and mitigate risks will help information system owners certify that a system is secure from theft, modification, and disruption or destruction of service. Most government agencies that are not part of DOD do not have classified information that pose a national threat if compromised. However, they do have sensitive information about the public and their own business processes that need to be protected. It not only makes sense to protect this information and certify the security for information systems, it is the law.

On December 17, 2002, President Bush signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA). That signing made the requirements identified in the Government Information Security Reform Act of 2000 permanent. In effect, that permanently codified OMB Circular A-130 into law and made it a requirement for each government system be certified and accredited prior to implementation and at least every three years after that.

A study of lessons learned from the first year under the Federal Information Security Management Act (FISMA) seems to pinpoint certification and accreditation (C&A) as the most important aspect of compliance.

The certification and accreditation process is a comprehensive analysis of the technical and non technical components of an IT system that needs to be completed before a system is moved into production. The analysis needs to be completed in an operational environment to determine that the controls and system artifacts have been incorporated in compliance with Federal, Departmental, and other pertinent regulations or laws. Some examples of non-technical controls to be assessed are: system security documentation, physical security, personnel security, and administrative procedures. Some examples of the technology that provide security are encryption devices/software, firewalls, access control, and audit tools. This is only a partial list of items to think about. The system being certified needs a list that matches its own security configuration and needs. Certification is a structured process that verifies techniques and procedures during the system's life cycle. It ensures that controls are implemented correctly and are effective to protect system confidentiality, integrity, and availability (CIA). Accreditation is the formal declaration by a designated approving authority that an information system is acceptable to perform in a prescribed security mode using a formal set of safeguards (Committee on National Security Systems CNSSI-4009, 2003). According to the Department of Defense, the certification and accreditation process can be broken down into four main phases: Definition, Verification, Validation and Post Accreditation.

This Definition phase establishes a comprehension of the Information System (IS) business case or mission, environment, and architecture to identify the security requirements and certification level of effort to accomplish accreditation. The goal is to conform on the system mission, operating environment, security requirements, C&A boundary, schedule, level of effort, and resources required. The creation of the System Security Authorization Agreement (SSAA), which is the binding agreement on the required level of security before system development begins, is included in the definition phase. The Verification phase supports the system’s compliance with the information security requirements and constraints identified and documented in the SSAA. The intention is to certify that the IS or components satisfy the security requirements. The

Validation phase reinforces compliance by an independent validation of the fully integrated version of the system to the operational requirements and security policy stated in the SSAA. The intent is to provide documented evidence to assist the DAA in making an informed qualified decision to permit approval for full system operation either by system accreditation or interim authority to operate (IATO). The Post Accreditation phase consists of activities that are used to monitor system management and operation within a level of acceptable residual risk. The system security management, change management, and annual compliance validation reviews are administered during this phase.

The C&A process can be tedious, costly and resource demanding. Ideally, the C&A process encompasses the entire life cycle of the system. It is a continuing, dynamic process. According to the Office of Management and Budget's (OMB) March 2004 report to the Congress, the authorized funding for IT security has increased from $2.7 billion in FY 2002 to $4.2 billion in FY 2003. However, a total of eighteen (18) agencies identified funding as a challenge to performing their certifications and accreditations. For example, the Department of Commerce (DOC) noted that their certification and accreditation was an expensive process and that in order to develop and implement its program, it had to reprogram and reprioritize internal funds and absorb costs in existing funding levels. In another case, the Department of Health and Human Services (DHHS) stated that because of limited funding, higher emphasis is placed on using funds to certify and accredit new systems as opposed to existing systems. The Department of Energy (DOE) also noted that funding was a challenge because security costs were not integrated into the overall life-cycle costs for all of its systems. Despite these and other concerns related to security cost funding, most agencies did not know how much they spent on certification and accreditation. For example, only 11 agencies could identify their actual or estimated costs for fiscal year 2003, which totaled $75.5 million for these agencies (GAO report on Information Security, 2004).

Nineteen (19) agencies surveyed also reported that they had encountered staffing challenges for their certification and accreditation activities that essentially consisted of the need for full-time staff with the appropriate backgrounds, specialized skills, and security clearances. In addition, thirteen (13) agencies reported challenges in providing

training to staff or officials responsible for certifying or accrediting agency systems (GAO report on Information Security, 2004).

As identified in the certification process, one of the most difficult, time consuming, and expensive task is to create and conduct the Security Test and Evaluation (ST&E) plan that is part of the Validation phase. The commitment to conduct and support ST&E requires considerable amount of manpower and financial resources from the agencies. Developing this plan is very challenging especially if it has to be done for the hundreds of systems owned by most Federal Agencies and military commands. One enormous task for creating the ST&E plan is to determine what non-Agency regulations and guides need to be included for testing, and then what types of tests should be scripted from them. Another major concern in the C&A process is defining system boundaries for numerous systems that need C&A. The demand on manpower resources to collect actual system environment information can be a daunting task. The C&A of high assurance systems would require more resources in the development of complex formal models and hiring of specialized skilled labor. An additional problem exists when storing and maintaining the System Security Authorization Agreement (SSAA) for so many systems, especially when the components in the SSAAs may be in different formats. The SSAA needs to be stored for future use -- According to Federal regulation; certification needs to be completed at least every three years for every system identified on an Agency's inventory.

In Special Publication 800-37, the National Institute of Standards and Technology (NIST) confirms that the cost of conducting certifications and accreditations on large numbers of information systems with varying degrees of complexity is a critical issue confronting existing agencies. NIST recommends as part of their solution is the promotion of reuse and sharing of security control development, implementation, and assessment-related information in the agency's agency wide information security program (GAO report on Information Security, 2004).

Another possible solution is to use an automated C&A tool that already has test scripts for Federal regulations and guidance together with having industry best practices already built in. This would mean using an automated C&A tool that can create a

repository of SSAAs, in a standard format for future use. Using an automated C&A tool that provides a standard, repeatable certification and accreditation process will greatly improve the current C&A process.

B. PURPOSE

The purpose of this thesis is to determine improvements in Navy Medicine's current Certification and Accreditation (C&A) process. This is done by determining whether the current Navy Medicine C&A policies and resultant efforts properly address the current C&A requirements confronting Navy Medicine networking professionals. A comparative evaluation of two automated C&A software solutions, namely Xacta and the Enterprise Mission Assurance Support System (eMASS), will be done. It will determine if the C&A software solutions can improve the implementation of the C&A process in Navy Medicine.

C. RESEARCH QUESTIONS

The following questions were used to guide the research and development of this thesis:

1. Are existing Navy Medicine Certification and Accreditation (C&A) policies in alignment with current Department of Defense (DoD), Navy Policy and federal government requirements?
2. Would the use of automated (C&A) software tools assist the Navy Medicine (C&A) process in obtaining system accreditation?
3. Would the use of automated (C&A) tools be a cost-effective means to address Navy Medicine C&A IA threats and vulnerabilities?
4. Would a consolidated and centrally-managed knowledgebase of (C&A) policies improve Navy Medicine current security posture?

D. SCOPE OF RESEARCH

This thesis will cover the vital aspects of Navy Medicine's current C&A policies. It will examine if Navy Medicine's current C&A policies and implementation efforts properly address current federal C&A requirements that are confronting Navy medicine IT professionals. It will also evaluate several C&A software solutions and examine how these solutions can improve the implementation of Navy medicine's current C&A policies within its claimancy.

E. METHODOLOGY

The methodology used for this research consists of the following steps:

1. Conducting a literature search of books, journal/magazine articles, CDROM systems, and other library information resources for the Xacta and eMASS C&A software solutions using key word queries.
2. Conducting a thorough review of Navy Medicine's current certification and accreditation process (DITSCAP) and resultant efforts in properly addressing federal and DoD requirements confronting Navy Medicine IT professionals.
3. Determining the information assurance (IA) controls satisfying the confidentiality, integrity and availability assurance level requirements for health care data based on the DoDI 8500.2, Information Assurance (IA) Implementation Policy.
4. Mapping the IA controls of DoDI 8500.2 to the DITSCAP SSAA and evaluating unmapped sections of the DITSCAP SSAA.
5. Exploring and contrasting the capabilities of two C&A software solutions Xacta and eMASS.
6. Determining how each software solution provides Navy Medicine IT management with the necessary tools, information and benefits to assist them in accomplishing a sound, informed, and timely certification and accreditation of their networks.

7. Interviewing other healthcare organizations and DoD agencies that may add value to this thesis.

8. Discussing the effect of having a consolidated and centrally managed knowledgebase of certification and accreditation policies in increasing Navy Medicine's current security posture.

The information that was collected for this thesis was obtained using the following methods:

1. Public Laws

- Privacy Act of 1974, P.L. 93-579,5 U.S.C. 552a (1974)
- Computer Security Act of 1987 P.L. 100-235 (1988)
- The Clinger-Cohen Act of 1996
- Management of Federal Information Resources (OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems", 1996
- Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA)
- Presidential Decision Directive-63 (PDD-63), 1998
- Gramm-Leach-Bliley Act of 1999, Public Law 106-102 (GLBA)
- Sarbanes-Oxley Act of 2002, Public Law 107-204 (SARBOX)
- The E-Government Act of 2002 (Public Law 107-347)
- Federal Information Security Management Act of 2002
- NIST Special Pub 800-37 – Guidelines for the Security Certification and Accreditation of Federal Information Technology System
- NCSC-TG-031 - Certification and Accreditation Process Handbook for Certifiers
- NCSC-TG-029 v1 - Introduction to Certification and Accreditation
- NSTISSI No. 1000 – National Information Assurance Certification and Accreditation Process (NIACAP)

2. DoD Policies and Guidelines

- DoD 5200.40 – DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
- DoD 8510.1-M – DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Manual
- DoD Directive 8500.1 – Information Assurance (IA)
- DoD Directive 8500.2 – Information Assurance (IA) Implementation

3. Navy Medicine Policies and Guidelines

- Military Health System (MHS) Information Assurance (IA) Policy / Guidance Manual

- Bureau of Medicine and Surgery (BUMED) Information Assurance Information Systems Security Policy Manual.

F. DISCLAIMER AND LIMITATIONS

The information that was used to assemble and analyze research findings is applied to satisfy the academic reporting requisites needed for the completion of a Master of Science Degree in Information Systems Technology from the Naval Postgraduate School. Interviews will be limited to the key Information Assurance Managers/Officers (IAM/IAO), account managers and staff of the Navy Medicine Enterprise Security Department - Technology and Information Directorate, IA and C&A Branch - Space Warfare Systems Command (SPAWAR) San Diego and Charleston, Telos Corporation and Information Assurance Technology Analysis Center. Additionally, research information or any other organizational data that was used within this research paper will be held in strict confidence and used solely for the indicated purpose.

The length of the academic term further limits the scope of the study and the efforts of this research may or may not accurately represent the other components of the United States Navy in regards to DAA, PM, UR, ISSM, ISSO and IAM/IAO or any other DoD representatives that fit the above mentioned titles or position.

II. BACKGROUND

A. INTRODUCTION

It is the main responsibility of the entire Federal Government to ensure the protection of all its information from unauthorized disclosure. This process of safeguarding all information in the Federal Government is called certification and accreditation. The certification authorities or certification agents enforce the certification and accreditation process.

A Certification Authority (Certifier) is the technical expert in the certification and accreditation process. The certifier is involved in the program's life cycle activities. It is the certifier's job to 1) confirm that the system or component determines and complies with the proper set of security requirements, 2) document and evaluate the residual risk and 3) submit a recommendation to the approving authority whether to allow the system or component to function thereby accepting the associated risk.

A Certification Agent is a Naval term describing a person who assists the certification authority. The certification agent's responsibilities are 1) to provide assistance in the development of the security engineering process 2) to assess and/or gather factual information that would be presented to the approving authority. This information will assist the approving authority to make a sound judgment whether to allow or disallow the continued operation of the system or component.

The Certification Authority and Certification Agent follow numerous Federal and DoD information assurance policies in enforcing the certification and accreditation process. The next section will briefly describe the information assurance requirements involved in the development of information security policy in the Federal Government, DoD and Navy Medicine.

B. INFORMATION ASSURANCE POLICY REQUIREMENTS

This section describes a few sources of information assurance requirements for Government automated information systems and components that DoD and Navy Medicine must satisfy. Governing Federal information assurance instructions and

directives define basic information assurance requirements. These requirements serve as a basis for establishing more defined administrative and technical security specifications, design and operational requirements.

1. Federal Government IT Security Requirements

a. Privacy Act of 1974, P.L. 93-579, 5 U.S.C. 552a (1974)

The Privacy Act of 1974 mandate all governmental agencies to protect all personal data generated and processed by automated information systems. This Privacy Act also directs the federal agencies to permit personnel to know what information is being managed. Updating inaccurate personal information is permitted by this Privacy Act. The Act focuses on the aspects of physical security policies, information management procedures, and desktop network oversight for systems that handle Privacy Act related data.

b. Computer Security Act of 1987 P.L. 100-235 (1988)

The Computer Security Act of 1987 went into effect on January of 1988. The Act requires all computer systems owned by the U.S. federal government that handle sensitive information to be managed by a security plan. The security plan must be tailored to address the specific management and usage of the system. The Act requires regular computer security awareness training for all federal employees, civilian contractors and other personnel directly involved in government sponsored programs.

c. The Clinger-Cohen Act of 1996 P.L. 104-106

The Clinger-Cohen Act is the combination of the Information Technology Management Reform Act (ITMRA) and the Federal Acquisition Reform Act (FAR). This Act was the result of the Federal Government's increased reliance on Information Technology and the resulting increased attention and oversight on its acquisition, management and use. The Act requires major federal agencies to establish the position of Chief Information Officer (CIO) who has the clear authority, responsibility and accountability for the Agency's information resources management activities and providing for greater coordination among the Agency's information. The Act also clarifies the responsibilities of the DoD CIO with those of the Military CIOs. The Military CIOs act as advisors to the DoD CIO, who in turn, advises the Secretary of

Defense in promoting improvements to the DoD work processes and supporting information resources.

The Act delegates to the DoD CIO all the responsibilities given to the head of the federal agency. The agency head together with the CIO ensures that the information security policies, procedures and practices of the agency are complete and current.

d. Management of Federal Information Resources (OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Systems", 1996)

The OMB Circular No. A-130 Appendix III, which was revised in February 1996, establishes a minimum set of controls to be included in Federal automated information security programs. It assigns Federal agency responsibilities for the security of automated information. It also links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123. The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A-130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives.

The OMB Circular No. A-130 focuses more on management controls, individual responsibility and accountability together with periodic awareness training, than focusing on technical and engineering controls. Federal agencies must ensure that risk-based rules of behavior and function are well established. All employees are to be provided with documented training and that the rules are enforced. It specifically requires agencies to manage and execute a program to make certain that all agency data collected, processed, transmitted, stored, or disseminated in general support systems and major applications are adequately secured. A formal risk analysis is no longer required in Appendix III. Instead, general risk assessments are addressed by risk-based management. The applications, vulnerabilities, threats, and safeguard effectiveness are considered major risk-based management factors. Ultimately, OMB, NIST, and NSA play a major role in assisting and providing guidance to the major federal agencies in order to improve their computer security posture. This appendix also requires a system security Plan (SSP)

and the appointment of a person responsible for the security of the system who has the authority to assume and accept the risk which is the Designated Approving Authority (DAA).

e. Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. 104-191

The HIPAA Security and Privacy Rule of 1996 was mandated by Congress to address the development of a national privacy law, security standards, and electronic transactions standards and provides penalties for standards violations and wrongful disclosures of health information. The Final HIPAA Security Rule was passed down by the Department of Health and Human Services with an effective date of 21 April 2003. Most HIPAA covered entities will have two full years until 21 April 2005 to comply with the standards. The HIPAA Security Rule particularly addresses the concern of the protection of electronic protected health information (EPHI). The confidentiality, integrity, and availability of electronic protected health information are the main goal of the HIPAA Security Rule. The HIPAA Security Rule further defines the steps and procedures for the proper handling and use of EPHI. As part of DoD and the Federal Government, compliance to the Final HIPAA Security Rule is required of all Navy Medicine facilities and health care providers. The establishment and enforcement of a set of security standards for securing certain patient health care information is the responsibility of all health care providers in the civilian and military treatment facilities. The definition of a health care provider is any provider of medical or other health services, or supplies, which handles or processes any health information in electronic form in conjunction with a contract or transaction for which a standard has been applied.

This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers. The use of the security standards is aimed to improve the Medicare and Medicaid programs, and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information. This Final HIPAA Security Rule implements some of the requirements of the Administrative

Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

f. Presidential Decision Directive – 63, (PDD-63), 1998

This Presidential Decision Directive focused on a national effort to assure the security of the country's critical infrastructures. The PDD-63 defines critical infrastructure as the physical and cyber-based systems essential to the minimum operations of the economy and the federal government. The critical infrastructures include, but not limited to, transportation, energy, finance, banking telecommunications and essential government services.

PDD-63 complements and expands other laws and regulations that address the security of our nations key cyber systems. PDD-63 requires an independent review of the security plans for protecting nation's critical systems. It requires the identification of the minimum essential infrastructure (MEI) that is critical to the operation of the economy and the federal government, including infrastructure interdependencies and the assessment of the MEI vulnerabilities across the major federal agencies. The PDD-63 claims that focusing on these vulnerabilities require evolutionary and flexible solutions that will cater to different sectors of society. The dynamic nature of the threats to the critical infrastructures require frequent assessments of their reliability and vulnerability. The protective measures and corrective responses must be robust, flexible and adjustable to the constantly changing threats.

g. The E-Government Act of 2002 P.L. 107-347

The E-Government Act of 2002 focuses on the critical relevance of information security and information assurance in E-Government. E-Government is defined as the use of information technology and the internet, together with the operational processes and people needed to implement these technologies, to deliver services and programs to constituents, including citizens, businesses and other government agencies. E-Government is aimed to improve the effectiveness, efficiency and quality of government services

The Federal Information Security Act of 2002 (FISMA), which is title III of the E-Government Act, has assigned the National Institute of Standards and Technology (NIST) the responsibility for the standards and guidelines. Federal agencies

will use the development of the NIST standards to classify information and information systems that they maintain. This is based on the intent of providing appropriate levels of information assurance according to a range of corresponding risk levels in order to recommend the suitable types of information and information systems that should be included in each category

h. Federal Information Security Management Act of 2002 (FISMA)

The FISMA of 2002 which was passed as title X of The Homeland Security Act and title III of the E- Government Act of 2002, mandates an increase of security for digital information and information systems in all federal offices. Under the supervision of The Department of Homeland Security, CIOs in every federal division must establish new stricter security measures replacing those in place under the old Government Information Security Reform Act of 2000 (GSRA). FISMA grants more responsibility and authority to NIST to develop and maintain standards for mandatory minimum information security and information assurance controls.

The head of the federal agencies and their respective CIOs are directed by FISMA to establish an information security program that would be managed by trained agency personnel who are responsible for the enforcement of training. The full integration of information security and information assurance into the current and future business practices is one of the main goals of FISMA.

The Designated Approving Authority (DAA), a senior management agency official, is required by FISMA to be responsible and accountable in authorizing each information system(s) in his agency for full operation using a formal certification and accreditation (C&A) process on the agency's system. All federal information systems are required to be certified using the certification and accreditation process. The proper implementation and operation of appropriate security controls in the system is the main purpose of the C&A process. FISMA also requires the regular certification and accreditation of continuously operating agency information systems.

The responsibility of providing information security safeguards on the scope and degree of damage as a consequence resulting from the unofficial access, handling, disclosure, disruption, alteration or destruction of data or information systems

belong to agency heads and their CIOs. It is required under FISMA that information security policies, practices and procedures are periodically tested and evaluated for effectiveness. The testing and evaluation has to be done with regularity depending on the associated level of risk but not less than annually so that effective implementation can be achieved. The standards and guidelines will provide consistency to the policies and procedures that are involved in detection, documentation and corrective action in response to an information security breach or mishap. These procedures also play a major preventive role in avoiding considerable denial of service or loss of data by mitigating the associated risks involved.

i. Gramm-Leach-Bliley Act of 1999 (GLBA) P.L. 106-102

The GLBA of 1999 replaced the Glass-Steagall Act of 1933 and allowed investment and commercial banks to consolidate and venture in the financial services industry. GLBA requires financial institutions to have a policy in place to protect the information from predictable threats and vulnerabilities in customer data security and integrity. GLBA compliance must be done whether the financial institution discloses nonpublic information or not. GLBA defines financial institutions as companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance.

The GLBA has two key rules, the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy Rule requires financial institutions to provide each customer with a privacy notice at the time the customer relationship is established and annually thereafter. The information collected about the consumer, where that information is shared, how that information is used, and how that information is protected should be thoroughly explained as required in the privacy notice. The privacy notice must also explain to the consumer of the opportunity to 'opt-out'. GLBA defines opting out when the client refuses to give permission allowing their information to be shared with affiliated parties doing business with the financial institution.

The Safeguards Rule require financial institutions to develop a written information security plan, practice and procedure that describes the company's contingency plan in preparation and in the continued protection of their clients' nonpublic personal information. The Safeguards Rule also applies to information of clients who are

no longer customers of the financial institution. This plan must include: (1) assigning at least one trained employee to properly manage the information security safeguards, (2) establishing a thorough and flexible risk management plan on each section or department that is handling and processing nonpublic information, (3) developing, monitoring, testing and evaluating the institution's program to secure critical customer information, and (4) evaluating and modifying the safeguards as needed while conforming with the changes in how customer information is collected, stored, and used.

The main intention of this rule is to do what current financial businesses should already to be exercising; which is protecting their client's information through a robust information security plan. The Safeguards Rule mandates financial institutions to focus closely at how they process and handle private customer information and to follow guidelines and procedures to do a risk analysis on their current existing operation. Every financial institution has to show continuous documented effort to achieve GLBA compliance since no process is perfect.

j. The Sarbanes-Oxley Act of 2002 (SARBOX) P.L. 107-204

Officially titled the Public Company Accounting Reform and Investor Protection Act of 2002, the SARBOX Act mandates financial institutions to improve the accuracy and reliability of their corporate and business disclosures in order to protect investors. The Act provides guidelines in the creation of a public company accounting oversight board, auditor independence, corporate and business responsibility and a more useful and accurate method of financial disclosure.

The SARBOX Act requires a report of the internal controls that a financial institution has implemented to make certain that compliance to SARBOX is achieved. It is required in Section 404 of SARBOX that Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) must regularly file the Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act periodic reports. The Securities and Exchange Commission (SEC) has provided rules and guidelines on the proper content of these reports. Management is required to provide documentation and do an evaluation of the effectiveness of their internal controls over their financial reporting. Companies and businesses must provide proof of their internal control assessment

program, specifically documentation of their control procedures regarding their information technology systems.

The security, accuracy and the reliability of systems that manage and report financial data is the responsibility of the company's CIO. Enterprise Resource Planning type systems are intimately integrated in initiating, authorizing, processing and reporting of financial data. An established information security plan to periodically assess the overall financial reporting process together with other important processes of the company is required to make sure SARBOX compliance is achieved. The Act requires a fundamental change in business operations and financial reporting. Even though the CEO and the CFO are responsible to provide the corporate financial reporting, it is the CIO who plays a major role in the signoff of financial statements because compliance to the Act will ensure that the company's information systems are providing correct data and analysis thereby making the financial reports more accurate and reliable.

2. DoD IT Security Requirements

a. DoD 5200.28-STD – Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)

The DoD 5200.28-STD was created by the National Computer Security Center (NCSC) to facilitate the widespread availability of trusted computer systems. In support of this goal the DoD Trusted Computer System Evaluation Criteria (TCSEC) was created, against which computer systems could be evaluated. The TCSEC was originally published on 15 August 1983 as CSC-STD-001-83. In December 1985 the DoD modified and adopted the TCSEC as a DoD Standard, DoD 5200.28-STD.

TCSEC is a collection of criteria that was previously used to grade or rate the security offered by a computer system product. No new evaluations are being conducted using the TCSEC although there are some still ongoing at this time. The TCSEC is sometimes referred to as "the Orange Book" because of its orange cover.

Under TCSEC, there are four levels that define criteria for trusted computer products. The four levels are A, B, C, and D. Level A, A1 being the highest, is

a system that can be proven through a mathematical model. Level B provides mandatory access control and require DoD clearance levels. Level C requires user log-on with a password discretionary access control and audit mechanism. Level D is a non-secure system.

Paragraph 2.2.3.2.1 of TCSEC requires department and section heads to validate the work they accomplished in their system documentation by testing their security protection plans and procedures. This security testing would examine and document vulnerabilities that would result in the easy bypass of their security mechanisms, allow isolation anomalies on resources, and permit unauthorized access or modification to authentication or audit information

b. DoDI 5200.40 –Department of Defense information Technology Security Certification and Accreditation Process (DITSCAP)

The DoD Instruction 5200.40 (DITSCAP) is a standardized process defined by DoD designed for managing risk. DITSCAP establishes a standard DOD-wide process, set of activities, general task descriptions, and a management structure to achieve the certification and accreditation of DoD Information Systems (IS). This process will preserve the Information Assurance (IA) and security posture of the Defense Information Infrastructure (DII), which is now the Global Information Grid (GIG), throughout the life cycle of the system.

The DITSCAP is designed to apply to any type of IT and any computing environment. It also applies to the acquisition, operation and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. The process can also be used for current existing systems certifications and other evaluated systems. It identifies four phases: System Definition, Verification, Validation, and Re-Accreditation, and uses weighted metrics to describe risks and their mediation.

There are four major role players in the DITSCAP process namely, the IT system program manager (PM), the Designated Approving Authority (DAA), the Certification Authority (CA) and the user representative. The agreement between these four managers is very important in the success of the DITSCAP process. These managers

work as a team to resolve crucial schedules, financial concerns, security, functionality, and operational issues. The System Security Authorization Agreement (SSAA) is the document that contains this agreement. The SSAA is used to provide guidance and document the results of the DITSCAP process. The main goal of the SSAA is to be the binding agreement on the acceptable level of risk and security that is required before a DoD system development program begins or modifications to the system are completed.

c. DoD 8500.1-STD – Information Assurance (IA) and DoD 8500.2-STD – Information Assurance (IA) Implementation

The DoD Directive 8500.1 mandates that "all IA and IA-enabled information technology (IT) products incorporated into DOD information systems shall be configured in accordance with DoD-approved security configuration guidelines". The directive also tasks the Defense Information Systems Agency (DISA) to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." The 8500.1 also requires the appointment of the DAA who is responsible and has the authority to accept the residual risk.

The DOD Directive 8500.2 implements the prescribed guidelines outlined in DoD Directive 8500.1. DoD Directive 8500.2 provides guidance in achieving the application of an integrated and layered protection on the DoD information systems by implementing policies, assigning responsibilities and prescribing procedures in accordance with DoD 8500.1

Directive 8500.2 requires the establishment of an information assurance program that evaluates security demands and performance thresholds. The development of the security design and configuration that conforms to a common architecture is the one objective of the IA program. Additional objectives of the IA program are implementing required controls or safeguards, the performing system tests and verification, and ensuring the appropriate use of life-cycle assurances such as configuration management.

This instruction clarifies many different aspects of DoD IA controls and mechanisms such as access control, configuration management and audit. Striking a fine balance between the importance of the information and supporting technology to DoD operations require risk management. The presence of documented threats and

vulnerabilities, the reliability of the end users and interdependent systems and the increasing demands for personnel and financial resources is vital in balancing the importance of the information and supporting technology to DoD missions. Per this instruction, these critical DoD missions are to be safeguarded from the documented threats and vulnerabilities, the untrustworthiness of users and interconnected systems, and the capability of IA solutions make risk management more complex (DoDI 8500.2, 2003).

Risk management is the process if identifying, measuring, controlling and minimizing or reducing the security risk incurred by a system to an appropriate level with the value of assets protected. It is a complex process because of the presence of outsider and more importantly insider threat. It is difficult to identify dynamic insider and outsider threat to a system or network and determining the vulnerabilities that may be exploited by the threats to ensure an acceptable level of security is achieved. However this instruction guides the major proponents of information security on how to develop the necessary countermeasures to eliminate or reduce vulnerabilities to an acceptable level.

3. Navy Medicine Command IT Requirements

a. Military Health System (MHS) Information Assurance (IA) Policy/Guidance Manual version 1.3 2003

The MHS IA Policy/Guidance was authorized by the Assistant Secretary of Defense for Health Affairs (ASDHA) and the Service Surgeons General. It was developed to address the consolidation of the MHS IT program development, management functions and personnel to improve efficiency and effectiveness. The policy guidance manual provides the requisite plans, procedures and direction needed to make sure that there are sufficient security safeguards that are enforced within the MHS to ensure compliance to the DoD's Defense-in-Depth IA strategy.

This guidance is the policy for all MHS centrally-managed Automated Information Systems (AISs) and networks under the authority of the MHS CIO. Additionally, this document is policy for the AISs and networks developed and operated by the TRICARE Management Activity (TMA) who is the lead agent for the MHS.

The stipulations in the manual covers all military, civilians and military contractors who are directly or indirectly involved in the management, design, development, operation, or acquisition or use of Tri-Service (centrally managed) AISs and networks. The manual also outlines the control of AISs and networks developed and operated by the TRICARE Management Activity (TMA). In addition, information systems that are Government Owned, Contractor Operated (GOCO) and Contractor Owned, Contractor Operated (COCO) that handle and manage DoD information are covered by the rules and regulations of this manual.

The occurrence of major or significant changes on DoD information systems or its operating environment will be addressed by risk assessments. The discovery of network security threats and vulnerabilities will be done by doing penetration testing during the C&A process. This can be done on a regular basis or as required by the MHS IA Program office. The MHS IA Program office will be in charge in conducting penetration tests on DoD information systems. The Program Office will coordinate these tests with the respective MHS component of the different Services. This will ensure that sufficient appropriate security measures that are being used by the Services.

The use of network vulnerability assessment tools on MHS components will be done to facilitate the identification of system and network vulnerabilities. Mission critical servers and networks will be annually evaluated by network vulnerability assessment tools. As part of the continuous C&A process, network vulnerability assessment software will be used on automated information systems and networks on a monthly basis. This assessment will be supervised by the MHS Component System Administrator and the Information Systems Security Officer.

Events that threaten the MHS Component security of operations such as unauthorized intrusions, denial of service attacks, and service disruption incidents will be handled by using a comprehensive process that will audit, detect, isolate and react to these events. The analysis of audit records on the information systems at individual command MHS sites is required to be done monthly or more frequently when necessary.

The information system owners of each MHS component will perform regular security monitoring and weekly reviews of system records as part of their C&A process.

b. Bureau of Medicine and Surgery (BUMED) Automated Information System (AIS) Security Program Policy Manual

The Bureau of Medicine and Surgery (BUMED) directs the worldwide medical and dental services and facilities maintained by the Department of the Navy. The mission of BUMED within the national defense structure of the United States is to safeguard the health of Navy and Marine Corps personnel in the following areas:

- Care and treatment of sick and injured members of the naval service and their dependents
- Training programs for BUMED personnel
- Continuing programs of medical and dental research
- Prevention and control of diseases and injuries
- Promotion of physical fitness of members in the naval service
- Care for on-the-job injuries and illnesses of civilian employees
- Supervision of the care and preparation for shipment and interment of deceased military members and of civilian personnel for whom the Navy is responsible

Given this mission, the inherent sensitivity of maintaining the BUMED information systems become a critical issue by concerns for the privacy and integrity of the patient's personal and medical information that is processed. Additionally, the availability of the health information systems that provide support in the delivery of quality access to care under Navy Medicine health care programs is also a critical management issue.

BUMED is headed by the Chief of the Navy Bureau of Medicine and Surgery, who also serves as the Surgeon General of the Navy (N093). The Chief of BUMED and his staff is responsible for the promotion of quality health care for the patient and professional responsibility for the patient's well being in Navy Medicine. The Chief of BUMED is responsible for providing high quality, economical health care to beneficiaries in wartime and in peacetime. BUMED provides highly trained Navy Medicine personnel that deploy with Sailors and Marines worldwide in providing critical mission support aboard ship, in the air, and on the battlefield. At the same time, BUMED Chief manages Navy Medicine's military and civilian health care professionals that are

providing care for uniformed services' family members and retirees at military treatment facilities around the globe.

In his/her other capacity as the Surgeon General of the Navy (SG), the SG is the head of Medical Resources, Plans and Policy division (N0931) at the Pentagon. The SG implements the Chief of Naval Operations (CNO) responsibilities for provision of centralized, coordinated policy development, guidance, and professional advice on health care programs for DON. The Navy SG oversees the direct and indirect systems for providing health care services to all beneficiaries in wartime and peacetime as authorized by law. He/she also acquires sufficient resources to provide these services.

The Navy Surgeon General's staff at N0931 is responsible for the coordination and implementation of the Navy SG participation for resource requirements in the Navy's Planning, Programming and Budgeting System (PPBS) process. The office of N0931 is responsible to develop balanced medical and dental programs within available resources, develop and evaluate plans and policy for medical support of general war and contingency operations. Under the leadership of the Navy SG, N0931 is tasked to develop and coordinate Navy and Marine Corps operational support requirements, establish and evaluate plans and policy in oversight and coordination of all aspects of deployable medical systems (DEPMEDS) and hospital ships. Furthermore, N0931 is directed to develop and evaluate policy in all aspects of medical research and development (R&D) initiatives consistent with operational support requirements and develop and assess legislative and policy initiatives involving issues related to Navy Medicine.

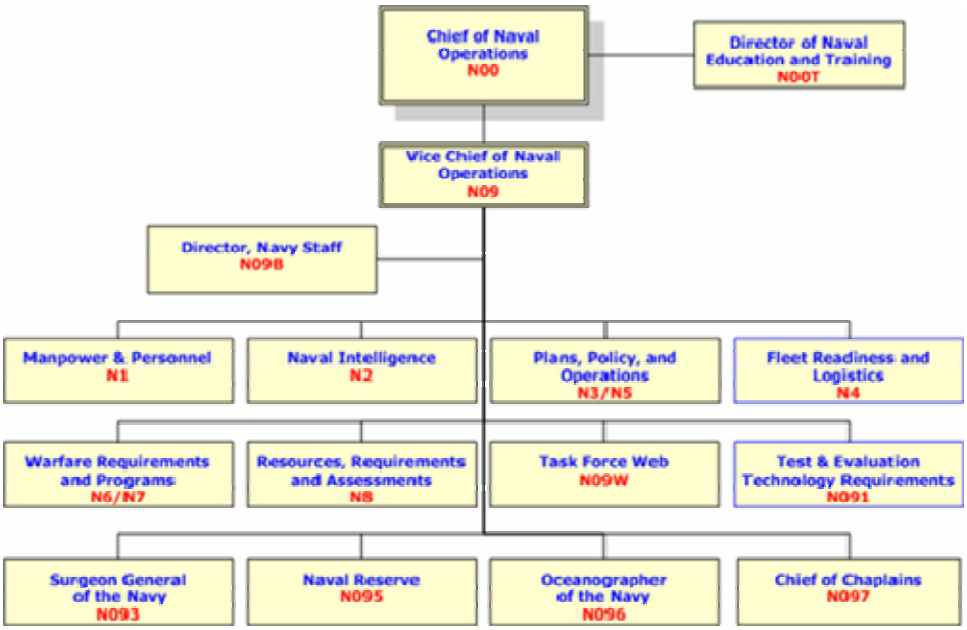


Figure 1. Chief of Naval Operations (CNO) Directorate
[From 21]

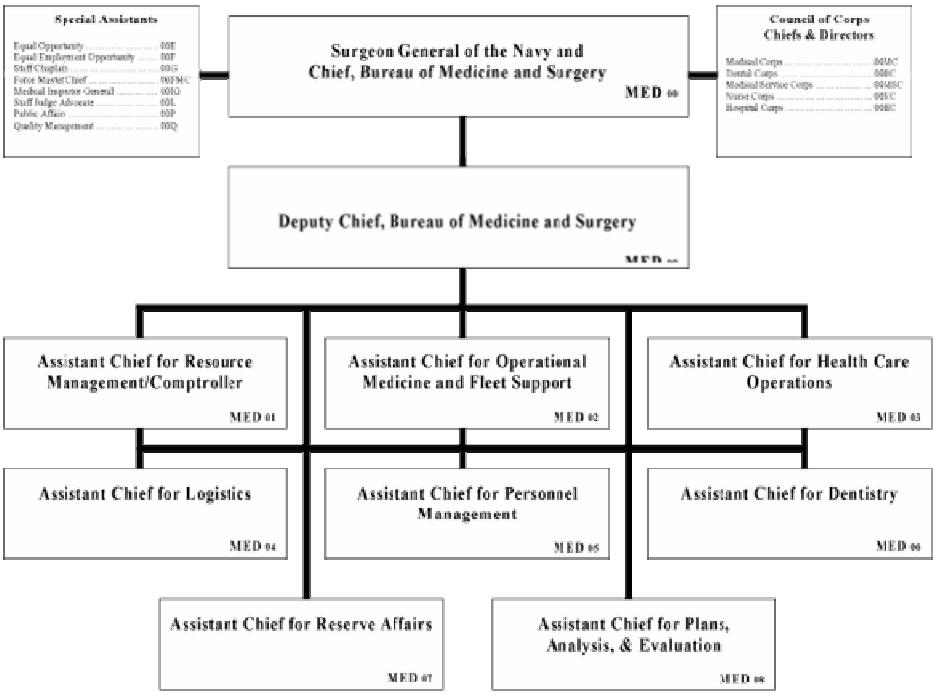


Figure 2. Chief of Bureau of Medicine and Surgery (BUMED) Directorate
[From 21]

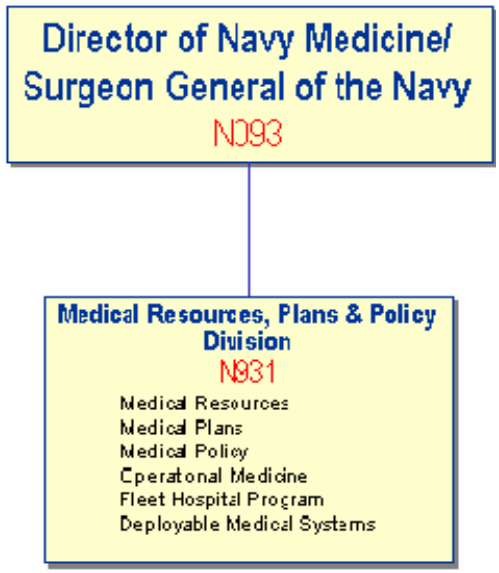


Figure 3. Surgeon General of the Navy (N093) Directorate [From 21]

The BUMED Information Systems Security Program requires that information security protection mechanisms are enabled to defend BUMED AISs against the threat of unauthorized modification, disclosure, destruction, and denial of service in the entire phase of the system life cycle. The information security policy for the protection of medical data, access to care services, and health resources related to development, maintenance and operations involving the systems and networks in BUMED's Claimancy 18 activities are established in this manual. Claimancy 18 activities are approximately 390 medical and dental activities and commands that report directly to BUMED.

The purpose of the BUMED security policy is to outline the security goals for Navy medicine patient and health provider data, medical services, and health related resources, i.e., those components of the BUMED systems and networks that require necessary privacy and security protection specially in accordance with the Health Insurance Portability and Accountability Act (HIPAA) regulations. The Program Managers, system designers, system administrators and helpdesk support personnel who are tasked to properly determine how to implement and enforce this security policy are

responsible for the specific implementation of security mechanisms, assurances and properties in the BUMED information systems.

The objective of this policy is to assure that each automated information system (AIS) has the appropriate level of security that is equal or greater than the risk and degree of damage that could be a consequence from the unavailability, corruption, unauthorized exposure, or modification of the information or information systems that maintains the data. It is in the BUMED security policy that all Privacy Act information and HIPAA patient identifiable data (PID) be secured and protected at all times. This includes the collection of all rules, procedures, and business practices that regulate the manner in which the medical and dental treatment facility handles, safeguards, and disseminates their patient and provider health information. The utmost protection of the confidentiality, integrity, and availability of the medical information in each system's level of security is a must.

The BUMED Information Systems Security Policy serves as a comprehensive compilation of information security guidelines with which BUMED systems and networks must ensure compliance. This document provides direction to the BUMED information security program as it applies through every phase of the information systems life cycle. This policy also serves as the basis for further improvements of information security requirements on increasingly complex medical data that is used by Claimancy 18 activities and commands, and more importantly, this policy actively upholds the continuous certification and accreditation efforts conducted on BUMED information systems and network infrastructure.

III. CERTIFICATION AND ACCREDITATION

A. THE CERTIFICATION AND ACCREDITATION PROCESS

The DoD's certification and accreditation process (C&A) is implemented in accordance with DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP). This instruction enforces the policies and guidelines as outlined in the DoDD 8500.1, "Information Assurance (IA)," Public law 100-235 (1987), and Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources." All components of the DoD, its military contractors, and other personnel involved in DoD information systems are required to comply under this instruction. Furthermore, milestone decision authorities (MDA) use this document in the acquisition of IT resources, and for the procurement, handling, and life cycle maintenance of any DoD system involved in the collection, storage, transmission, or processing of different types of information.

The goal of DITSCAP is to implement a systematized methodology to DoD's certification and accreditation process. This document provides guidance in specifying necessary steps and procedures required to be addressed when evaluating a system for C&A.

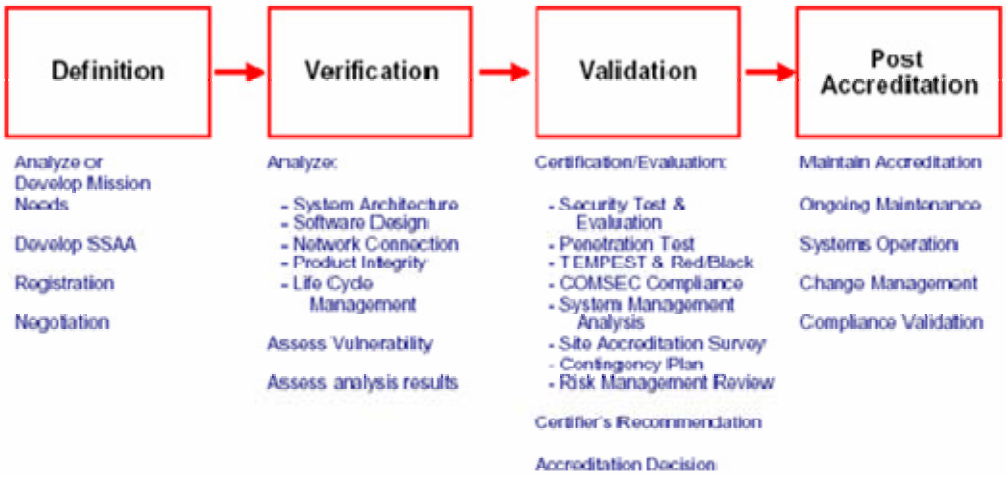


Figure 4. DoD Information Technology Security Certification and Accreditation Program Overview
[From 3]

The certification and accreditation process of is implemented in four phases. These phases are Definition, Verification, Validation, and Post Accreditation. The first phase in the process is Definition. The first phase focuses on comprehending the information system business case or system mission. The objective of the definition phase is to determines and agree on the system boundary, operating environment, security requirements, schedule, resources and the level of effort required. The creation of the initial draft of the System Security Authorization Agreement (SSAA) is incorporated in this phase.

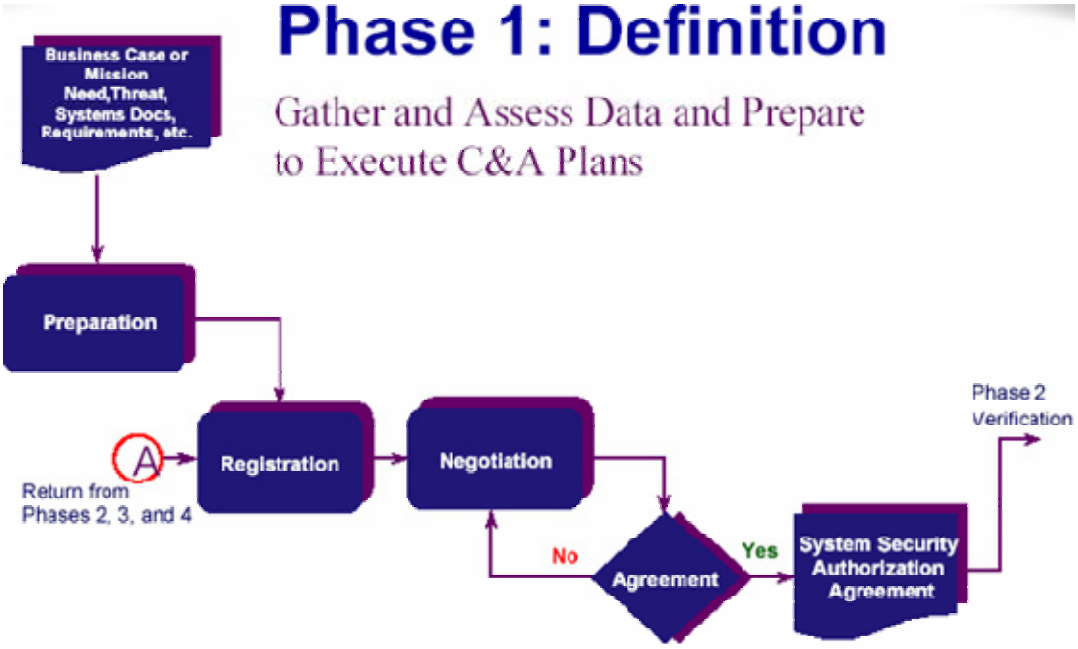


Figure 5. DITSCAP First Phase Activities [From 3]

There are three main activities in the definition phase. They are preparation, registration, and negotiation activities. The collection of all documentation and information involved in the system to be certified and accredited is accomplished in the preparation activity. The initiation of the risk assessment process involving the identification of security requirements, system boundaries and level of effort to ensure completion of the C&A process is accomplished in the registration activity. The negotiation activity confirms that the initial draft SSAA appropriately defines the level of effort for the system. This activity assures that the main proponents and other members of

the C&A team are thoroughly familiar with their roles and responsibilities in the DITSCAP process. The business mission and system information, operating environment, system security requirements, C&A boundaries, acknowledged security problems or discrepancies, and other security-relevant information are incorporated in the SSAA.

The level of the certification effort is established by analyzing the business or system mission, functions, security requirements, architecture, and final end users. Documentation of this data will facilitate the analysis of the degree of confidentiality, integrity, availability and accountability that is deemed appropriate for the system. The level of certification effort is dependent on the level of confidentiality, integrity, and availability that is required of the system. The availability of this information provides the appropriate amount of assurance that the system will have full system functionality as defined in the system and security requirements It is necessary that the main proponents of the C&A process have full understanding that appropriate level of assurance necessary for the system requires the corresponding mandatory safeguards needed for system operation. The assurance of confidentiality means that the information is accessible only to those authorized to have access and that it is assured from destruction or corruption. The application of access control, cryptography, object reuse, physical security, emissions security techniques, administrative and engineering controls are several safeguard mechanisms that are used to enforce confidentiality. These protection mechanisms assist in preventing unapproved user control, hijacking, and electrical transmission. The preservation of integrity is accomplished by preventing the modification and deletion of information by unapproved users. Reliable integrity assurance mechanisms are access control, digital signatures, configuration control, and physical security. Availability is the degree to which the operation, data, infrastructure or system needs to be available as accessed by authorized users. The avoidance of denial of service attacks by unauthorized users is the main goal of availability. Several security mechanisms used to safeguard availability are restriction of access control, use of data backups and archives, modularity, redundancy and operations security (OPSEC).

There are four certification levels of effort in the DITSCAP. The determination of the certification level of effort will dictate the amount and degree of analysis that will be done for the system. Selecting the appropriate certification level of effort is critical in

ensuring the proper implementation, security and requirements for the system. The certification level of effort indirectly determines the amount of resources that will be used in providing relevant information to the main C&A proponents. The Designated Approving Authority (DAA) will assess and evaluate the relevant data that is required to determine an informed accreditation decision. In each certification level of effort, a considerable amount of verification analysis is required to assure that the system behavior demonstrated conforms to the requirements definition specifications. Level one requires the completion of the minimum security checklist. This checklist can be found in Appendix 2 of the DoD 8510.1-M (DITSCAP Application Document). This minimal security activity checklist documents that the detailed concepts of system architecture, design (software, hardware and firmware), network connection rule compliance, integrity, life-cycle management, vulnerability assessments, system management, security test and evaluations, penetration testing, TEMPEST, and COMSEC requirements to the system have examined and reviewed to the fullest applicable level. The completion of the minimum security checklist is required in levels two, three and four. However, an independent, in-depth or extensive analysis of the system is also required. Determining the required analysis level of effort is accomplished by selecting alternatives for each of the key security-relevant characteristics that describes the system. Each characteristic has an assigned corresponding weight which is entered in the right column. The total of these weights is used to determine the appropriate certification level.

Table 1. Certification Level of effort
[From 2]

Level	Certification Level of Effort	Description
1	Minimum Security Checklist	Requires the completion of the minimum security checklist. The system user or an independent certifier may complete the checklist. This checklist can be found in Appendix 2 of DoD 8510.1-M, the DITSCAP Application Document.
2	Minimum Analysis	Requires the completion of the minimum security checklist and independent certification analysis as defined in the verification and validation phases.

3	Detailed Analysis	Requires the completion of the minimum security checklist and more in-depth. Independent analysis as defined in the verification and validation phases
4	Extensive Analysis	Requires the completion of the minimum security checklist and the most extensive independent analysis as defined in the verification and validation phases.

Table 2. System Characteristics and Weights
[From 2]

Characteristic	Alternatives and Weights	Weight
Interfacing Mode	Benign (w=0), Passive (w=2), Active (w=6)	
Processing Mode	Dedicated (w=1), System High (w=2), Compartmented (w=5), Multilevel (w=6)	
Attribution Mode	None (w=0), Rudimentary (w=1), Selected (w=3), Comprehensive (w=6)	
Mission-Reliance	None (w=0), Rudimentary (w=1), Selected (w=3), Comprehensive (w=6)	
Availability	Reasonable (w=1), Soon (w=1), ASAP (w=3), Immediate (w=6)	
Integrity	Not-applicable (w=0), Approximate (w=3), Exact (w=6)	
Information Categories	Unclassified (w=1), Sensitive (w=2), Confidential (w=3), Secret (w=5), Top Secret (w=6), Compartmented / Special Access (w=8)	
	Total of all weights	

During phase I of the process, a decision as to the certification level will be made and it is important to understand each factor of that decision. In determining the certification level, many factors are considered and given weights, these weights are added together to give the appropriate certification level. In some circumstances, the characteristics of a particular category might dictate a higher certification level than that indicated by the total weights. Among the four certification levels, the weights that identify each level overlap each other and might be an area of possible contention. This means that a level one or two, level two or three, level three or four certification could be required if the total weights fall into one of those ranges. This is where the negotiating

aspect of DITSCAP is employed. The main proponents of the C&A must collectively agree on the certification level of effort to be used on the C&A. This agreement is normally accomplished with the least amount of grief and anxiety among the C&A proponents. The proponents of the C&A have some latitude to add their own subjective opinion. This emphasizes the need for the proponents of the C&A to be equally prepared and experienced in order to know how to assist the DAA in making the appropriate decision. The DAA is also responsible for defining the accreditation requirements, obtaining a threat assessment for the system, assigning a Certifier to conduct the vulnerability and risk assessments, supporting the DITSCAP tailoring and level of effort determination, and approving the SSAA. The Certifier as well as the certification Team will support the DAA in any way they can with his/her responsibilities.

The specific certification level of effort and documentation for certifying a system is at the discretion of the DAA. The decision of the DAA can be affected by several factors that can increase or decrease the degree of certification testing, analysis and documentation required. The degree of interconnectivity with other systems, the projected life expectancy of the system and the associated cost and investment on achieving the full level of certification effort associated with the C&A. The DAA will be the management official that will be responsible for accepting the risk.

Table 3. DITSCAP Levels of Certification and Weights
[From 2]

Certification Level	Weight
Level 1	If the total of the weighing factors are < 16
Level 2	If the total of the weighing factors are < 12-32
Level 3	If the total of the weighing factors are < 24-44
Level 4	If the total of the weighing factors are < 38-50

The determination of the system's security requirements are outlined in Task 1-5 of the DITSCAP. The proponents of the C&A must examine the directives and security requisites to establish the applicable security requirements for the system. The certification team will focus on a section of the DODI 8500.2 for basic IA controls that

would subsequently be parsed into security requirements statements. The resulting security requirements will then be written into the Requirements Traceability Matrix (RTM) to facilitate the remainder of the C&A process.

The RTM is usually in a spreadsheet format with an additional comment block for more specific details. The RTM conforms with the requirements through the System Security Requirements Specification (SSRS), and maps to the specific sections of the in the Certification Test and Evaluation (CT&E) procedures and the Security Test and Evaluation (ST&E) procedures where the requirement is tested. The type of assessment is indicated in the "Evaluation Method" column of the RTM. DITSCAP uses I=Interview; D=Document Review; T=Test; O=Observation. The next block shows whether the requirement was met or not. The progress of the certification effort throughout the entire process is monitored by the C&A proponents by using the RTM. The RTM provides an excellent overview of the entire effort at the completion of the C&A and gives a quick snapshot of the completed and in-completed requirements.

Table 4. Requirements Traceability Matrix
The Chain of Traceability from Policy to Test Procedure
[From 3]

IAC Description	Source Document	Policy ID	Test Method (I, D, T, O)	Test Procedure ID	Comment
An annual IA review shall be conducted that omprehensively evaluates existing processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations	DoDI 8500.2 Attachment 1 to Enclosure 4	Availability AV-1 AV-5 AV-7	I	TP-2	
The DoD information system security design shall incorporate best security practices such as single sign-on, PKI, smart card, and biometrics.	DoDI 8500.2 Attachment 1 to Enclousre 4	Integrity IN-1 IN-3 IN-6 IN-8	I D	TP-4 TP-5	

At the conclusion of the first phase, the C&A proponents will have a full understanding of the resource requirements needed in the C&A process. An agreement on the level of certification has been reached, as well as the requirements that will be tested and verified in the second phase. The main C&A proponents sign to acknowledge the SSAA with their signatures meaning that they have reached an agreement to satisfy and comply with these requirements.

The second phase of the process is Verification. This phase begins with updating the SSAA as new system changes in the security requirements occur. The analysis of the system architecture, software design, network connection rule compliance, products to be integrated into the system, life-cycle management, security requirements validation procedures, and vulnerability assessments are included in this phase.

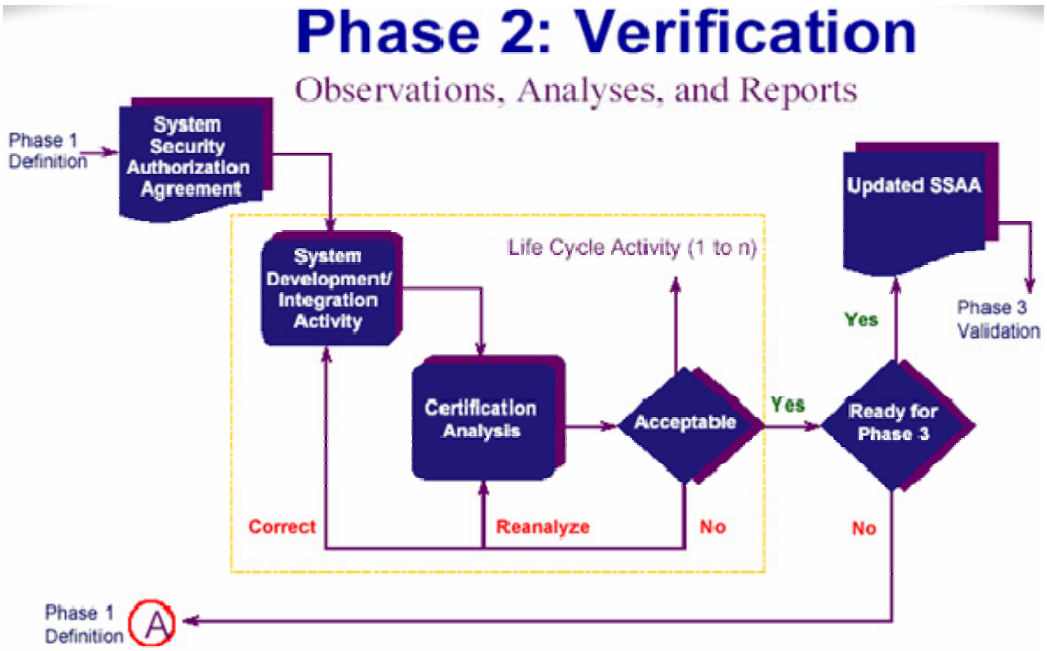


Figure 6. DITSCAP Second Phase Activities
[From 2]

It is important that all the C&A proponents are aware of any adjustments made to the system because any change or adjustment can influence the scope of the C&A effort. The proponents must keep monitoring these changes to prevent failure in completing

their C&A process. The C&A team must not think that they have a limited role while the exact opposite is true. All the C&A proponents must be proactively involved in each phase as it implemented and enforced throughout the whole C&A process.

The C&A process and security requirements analysis is performed to ensure adequacy and correctness. The analysis is also used to verify the relevance to the C&A process and conformity to the SSAA requirements. The C&A analysis will also confirm that the system design implementation satisfies the SSAA stated requirements as well as ensure the proper operation of the critical security components of the system. As the dimension and difficulty of the system under development changes so will the security requirements and the C&A effort.

The certification process is examined to make sure that it is adequate. This evaluation of security requirements can result to the addition or deletion of requirements that were discussed in Phase One. The DITSCAP application manual lists seven initial certification tasks to be completed during the verification phase. They are (1) System Architecture Analysis, (2) Software Design and Analysis, (3) Network Connection Rule, (4) Integrity Analysis of Integrated Products, (5) Life Cycle Management Analysis, (6) Security Requirements Validation Procedures Preparation and (7) Vulnerability Assessment.

The Certification Test and Evaluation (CT&E) is done to focus on a system's security assessment irregardless of its business setting. This evaluation is often conducted in research laboratories. This allows for a more comprehensive and thorough testing of the system. It is during the CT&E that the security features in the system are verified with its technical security requirements. Generally, the Security Test and Evaluation (ST&E) occurs after the CT&E. This allows the system installation, integration and configuration for secure operations to be verified by the Certifier. It also sets up the opportunity for the Certifier to evaluate the security of the business setting and examine the capability of the ST&E test coverage. There are two pre-requisites before conducting the CT&E. First, the security features of the system must have configuration management control from the start of the CT&E up to the conclusion of Phase three. Second, there should not be any expected system changes before submission of system deliverables.

At the completion of the certification analysis, a well documented security specification, a comprehensive test plan and procedures and a document assuring that all network and network interface requirements have been determined, is prepared. The certification analysis outcomes are deliberated at the conclusion of each development stage. During the Verification Phase, the Task Analysis Summary Report and the evaluation and determination of system certification readiness is developed. The Task Analysis Summary Report uses the information from the SSAA, results from each certification task, discrepancy reports, system architecture and software design, and independent validation and verification reports as sources of input for each certification task. The output of the Task Analysis Summary Repot shows the record of findings, an evaluation of vulnerabilities discovered during system evaluations, a summary of the analysis level of effort, a summary of tools used and results obtained during the certification tasks and recommendations.

Before proceeding to the actual Validation Phase, the knowledge that the system is ready to be certified has been determined. This means the system is assumed ready for testing of the fully integrated system in its hardware and software environment. System evaluation was done at each development step and inconsistencies and discrepancies discovered were identified by the C&A team and submitted to the main proponents of the C&A. This will enable the main proponents of the C&A to make necessary corrections or modifications.

The DAA will be informed of any additional resources needed in the C&A process. Significant changes to the extent of the certification effort will result to require additional resources.

During the Verification Phase, the regular review of the system to ensure its accordance with the SSAA is done by the DAA. The process of overseeing the system evaluation as well as analyzing the SSAA to ensure correctness in describing the system, threat, environment, security requirements, vulnerabilities to the system, and all other conditions in which the system will be operating is also the responsibility of the DAA.

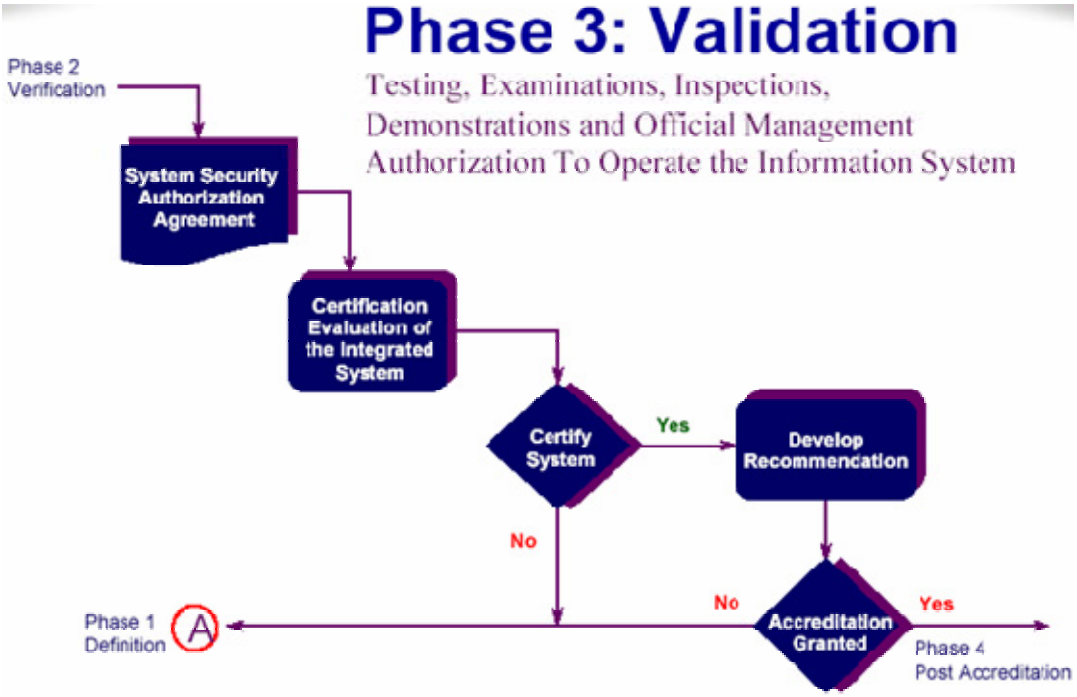


Figure 7. DITSCAP Third Phase Activities
[From 2]

The third phase in the process is Validation. The validation of findings discovered in the Definition and Verification phases that contributed to the inception of an acceptable system. A system that performs within the specifications as stated in the requirements definition, and demonstrates the desired functionality and operability within an acceptable level of residual risk.

During this phase it is imperative that the certifier and the C&A team closely collaborate throughout the entire C&A process and not only in one phase. The certifier and the team are major players in getting the C&A process to this point. They have provided critical input in determining the level of certification, determined the requirements to be tested on the system and provided valuable oversight to the system development process.

By this time, the system to be accredited has already been integrated, and is awaiting the official accreditation decision. Again, the SAA will be reviewed, the integrated system will be evaluated, and the final accreditation decision will be made. At

the center of this phase is the System Test and Evaluation (ST&E). This set of actual test procedures are a detailed descriptions of the testing of security features to be performed during development. The ST&E is a detailed vulnerability analysis that is done during phase three. The goal of ST&E is to examine and analyze the security protection features required to safeguard a system as it is related to its business setting. The ST&E is a collection of actual test procedures used to determine the technical and non-technical security design features of the system. It is during the ST&E that the enforcement of important security features namely, intrusion detection systems, audit trails, contingency planning, physical and technical features of access control, anti-virus programs, automated security tools, procedures and policies are examined for conformity to the defined security design requirements. The C&A team makes every attempt to address and rectify security related discrepancies or vulnerabilities that are discovered during the ST&E. The outcome of the ST&E is an itemized report containing evaluation results, and data pertaining to the degree of residual risk. The extent of residual risk that remains after the security mechanisms have been enforced is called residual risk. It is very important that the Certifier, who is an experienced IA professional, properly compile the Test Plan and Procedures report. The report will be proof that the system had undergone meticulous testing with documentation that was proper analyzed. This report will assist the DAA in deciding the acceptable degree of residual risk to allow full system operation. The key in this phase is the residual risk assessment.

The ST&E is performed during the evaluation to ensure that the security controls for the system are correctly implemented and working efficiently. The procedure describes the specific requirement based on the RTM. It also states the intention of the test, and outlines the success criteria. The DITSCAP application manual is a good source of examples on the proper format for each of the test procedures. Penetration testing, verification of TEMPEST compliance, communications security, system management analysis, site accreditation survey, evaluation of contingency plan and a risk management review are other testing areas required under DITSCAP.

In addition to the ST&E, the C&A team needs to provide other pertinent documents. The Risk Assessment Report (RAR), Certification Evaluation Report (CER), and the Certification Statement. The CER contains the result of the certification testing

(ST&E). The CER also presents the comprehensive security test principle, the specific testing procedures and test results with comments. The RAR provides an in-depth analysis of the areas that were not successful in the ST&E. An analysis of threats, vulnerabilities and risk outcomes to the system are documented in the RAR report. For identified high risk concerns, the RAR describes the security weakness and defines the associated vulnerability. The RAR contains suggested countermeasures with corresponding risk reduction explanations.

The results, observations and evaluations in this phase and the previous phases are compiled in a report for the DAA. The Certifier must disclose his observations and system accreditation recommendations to the DAA. Risk Assessment and Certification Evaluation Reports are developed and the certification statement is prepared. If the security requirements outlined in the SSAA were satisfied by the system then system certification is issued by the Certifier. This certification confirms that the system has properly complied to the system security requirements. Otherwise, if discrepancies remain yet the mission criticality requires system operation at an acceptable level of risk then the Certifier can issue an interim approval to operate (IATO). Correcting these deficiencies have a fixed time limit and are documented in the SSAA.

The certification statement is the report to the DAA on the results of the certification testing. This report will include the recommendation to accredit the system or not, or to grant an interim approval to operate (IATO). A return to phase one renegotiation, then phase two and three would be the recommended solution if the system still contains extremely high risks. This ensures repeatability is achieved in the C&A process. If the DITSCAP process was diligently followed by the C&A team and security experts then it is highly unlikely that a recommendation to disapprove an accreditation will ever happen.

The documented system information and recommendation from the Certifier is now used by the DAA in reviewing the SSAA and arriving at a final accreditation decision.

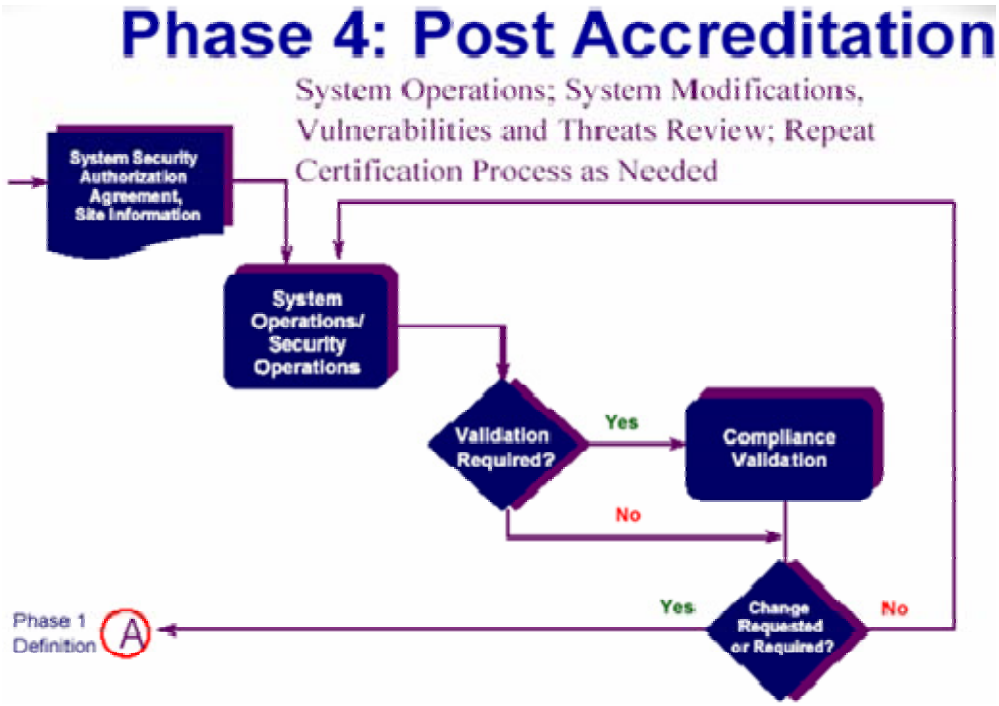


Figure 8. DITSCAP Fourth Phase Activities
[From 2]

The fourth and final phase in the process is the Post Accreditation Phase. At this point the system has already been accredited and follows process activities that will operate and manage the system while maintaining an acceptable degree of residual risk. A system that is operating under an IATO will have to correct the system deficiencies that were discovered in phase three within a fixed amount of time. After the system is integrated into the operational computing environment and accredited, the system is monitored regularly to ensure that there are no significant changes to the configuration or environment that might affect the confidentiality, integrity or availability of the information contained. This monitoring is performed throughout the system's lifecycle. A regular review to track system changes must be done to ensure that the system's threat level will remain unaffected. Changes made must be controlled to preserve the stated configuration management requirements. Any changes made in the system can result in a change in the system's security posture. Threats to the system mission, architecture, security policy, system risk, operational mode, audit results and sensitivity levels are some aspects that may cause change. The accreditation of the system is highly dependent

on the system configuration and the manner in which the system interfaces with its hardware and software components. Suggested future changes must be thoroughly reviewed by the proponents of the C&A to prevent the invalidation of the accreditation decision. The mitigation of possible system challenges as a result of system architecture, policy or design adjustments are handled using the risk management review process.

It is essential that effective risk management review is conducted at this phase. A critical step in ensuring system security is the periodic evaluation of changing system threats. These system evaluations mitigate risk and provide valuable data in the system performance analysis. The continuous system operation within an acceptable level of risk is always maintained especially when the system security design and architecture is assessed against the security requirements defined in the SSAA.

It is the responsibility of the Information System Security Officers (ISSO), the DAA, and system operators and administrators to maintain the security posture of the system. Re-accreditation will include the same procedures that were used to complete the original accreditation. However, valid sections of the original accreditation documentation need not be updated. Conducting on-site interviews enforces the effectiveness of a strong awareness program and information security training. It would also be recommended to the C&A team to conduct random spot checks on security procedures that were previously tested.

1. Duties and Responsibilities

The main proponents in the certification and accreditation process are the DAA, Certifier (CA), Program Manager (PM) and User Representative. The Information Assurance Officer (IAO) formerly known as the ISSO, the Information Assurance Manager (IAM) formerly known as the ISSM and the System Administrator are privileged users with IA responsibilities that support the main proponents of the system's C&A process. It is very important that the DAA, PM, user representative, IAO, IAM and system administrators all perform their jobs to the best of their ability. This will ensure that re-accreditation after three years will be less stressful and there is greater assurance that the system life cycle will be more secure. An informed proactive posture to information security certification and accreditation will maintain public and Government

trust in the agency's ability to conduct business while avoiding undesirable and unnecessary information security mishaps.

DITSCAP allows other roles to be added to support the overall decision process and mission. DITSCAP permits the establishment of certification teams under the certifier's supervision to extend assistance to the certifier in the performance of the actual security testing. The Program Manager and IAO are major players in the C&A process. Each of these roles greatly affects each phase of the process. These roles are responsible for deciding the range of the effort as it pertains to the system mission, resources, architecture and environment. The members of the C&A team must collaborate to ensure that the project stays on schedule, complies with design implementation, and adequately handle possible threats to the system. During Phase one of DITSCAP, it is very important that all roles in the certification effort come together and collectively expound on the security requirements, scope, and certification level of effort. This exchange of ideas should result to a final consensus by the members of the C&A team.

The DAA is the senior management individual who is responsible for making sure that the system functions within an acceptable level of risk. The DAA is the person with the positional authority to fully accredit the system. As a member of the agency's upper management and it is their responsibility to evaluate the agency mission and available resources for the system to be accredited. The DAA has to have the authority to accept the risk. The extent of acceptable residual risk depends on numerous factors, most important is the mission criticality. The accepted residual risk may be significant depending on the importance of the mission. It is pertinent to comprehend that the management has the ultimate decision and many internal and external factors may influence this decision.

The Certifier is the person responsible for making sure that the DAA receives sufficient pertinent information concerning the involved risks. The Certifier is the technical expert in the certification process and provides the necessary technical information needed by the DAA. It is the Certifier's prerogative to execute the C&A process with a team. The Certifier ensures that the proper documentation of the security requirements noted in the SSAA. The appropriate level of residual risk is recommended

by the Certifier. The Certifier develops the accreditation package and submits the accreditation recommendation to the DAA.

The Program Manager manages each aspect of the system from the original concept, to the development, implementation, and system maintenance. The program manager is responsible for the system throughout its entire lifecycle, and is responsible for ensuring the security requirements are implemented correctly. The PM has the ultimate responsibility for the overall acquisition, evolution, incorporation, alteration or operation and maintenance of the system. The PM ensures the use of cost-effective IA standards to the program by using appropriate resources and setting priorities.

The User Representative is concerned with the system's confidentiality, integrity, availability, access, functionality and performance as it relates to the ultimate mission of the system. The user representative represents the operational interests in the system user community and assists in the certification and accreditation process by helping to define the system operations and functional requirements. He/she provides input for system mission use requirements and SSAA input in the data sensitivity and end-user functionality sections.

Information Assurance Manager (IAM) is operational system's technical security expert. He/she is an advisor to the DAA. The IAM is responsible for creating and managing the information system's security program. The IAM performs tracking and incident reporting, system vulnerability assessments, routine audit trail reviews, and regular reporting of systems security condition. The IAM is a key player in the establishment and authorization of the SSAA. He/she facilitates and oversees the performance of numerous IAOs (CJCSM 6510.01, 2004).

The Information Assurance Officer (IAO) is responsible for monitoring and maintaining the security of the system as defined by the SSAA, as well as ensuring that the system follows all security requirements as stated in the documentation. The IAO reports the security status of the IS to the IAM, as required by the DAA. The IAO maintains the System Security Plan (SSP) and ensures TEMPEST measures are enforced. In addition, the IAO conducts user training and awareness activities under the supervision of the IAM (CJCSM 6510.01, 2004).

The System Administrator (SA) is responsible for the proper operation, maintenance and disposition of the systems in agreement with the security policies and practices as defined in the C&A package. The SA enforces proper authorization, security clearances, need-to-know for all users before granting access to the systems. He/she reports all security related incidents to the ISSO, maintains and documents configuration management (CM) for all security relevant IS assets. The SA is also responsible for the monitoring of system recovery process and the proper restoration of the systems security features and procedures when needed.

The management of each aspect of the system life cycle starting from its original concept, to the development, implementation, and system maintenance is the Program Manager's responsibility. The program manager is responsible for the system throughout its entire lifecycle, and is responsible for ensuring the security requirements are complied and properly implemented.

B. XACTA CERTIFICATION AND ACCREDITATION SOFTWARE SOLUTION

1. System Name and Identification

System Name: Xacta Information Assurance (IA) Manager Enterprise Edition V4.0

System ID: Xacta IA Manager Enterprise Edition V4.0, Xacta Assessment Engine.

2. System Description

The Xacta IA Manager Enterprise Edition is a private-owned, Commercial-off-the-Shelf (COTS) based information security risk management software application. With Xacta IA Manager, the C&A team defines the network or system configuration and the environment in which it operates, and the application automatically engages the appropriate security requirements according to government and/or industry best practices. The software then automatically generates the appropriate test procedures, processes the test results, produces a risk assessment, and allows the user to automatically publish a complete C&A package, including all appendices, in accordance with the National

Institute of Standards and Technology (NIST), the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), the National Information Assurance Certification and Accreditation Process (NIACAP), or the Director of Central Intelligence Directive (DCID). Through the software's automation of these formal processes, organizations can validate their compliance to Government and DoD mandates, such as the Federal Information Security Management Act, Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, Sarbanes-Oxley, Privacy Act of 1974, DITSCAP and DCID 6/3. In addition to traditional security assessment and compliance, the software provides Continuous Assessment of the network and system security posture to ensure emerging threats are mitigated prior to an attack.

The Xacta IA Manager is a comprehensive solution for IT security administrators that manage risk, sustained compliance, vulnerability management and remediation through the use of cutting edge automated security methods. It merges the industry-leading compliance and risk assessment features with effective mission process integration technology to create a centralized security management platform that facilitates and enhances compliance assessment, constant risk and routine compliance management, and security process enforcement.

After being acquired by numerous federal agencies and commercial enterprises, Xacta IA Manager enables its users to enforce continuous risk and security compliance as well as initiate corrective actions automatically that are necessary in the protection mission essential systems.

The Xacta IA Manager was developed and released by Xacta Corporation, a Northern Virginia-based security software company. It was originally developed as Xacta Web C&A to address the need for standards-based security assessment and was further developed to Xacta Commerce Trust, a continuous enterprise risk management product. By leveraging Xacta Web C&A's and Xacta Commerce Trust's architecture and the knowledge base the company created to support the system certification and accreditation needs of the federal marketplace, Xacta developed the IA Manager which is enables information security-conscious corporations and organizations to achieve more than

minimum compliance and demonstrate a more proactive, enterprise-wide posture in conducting and executing risk management.

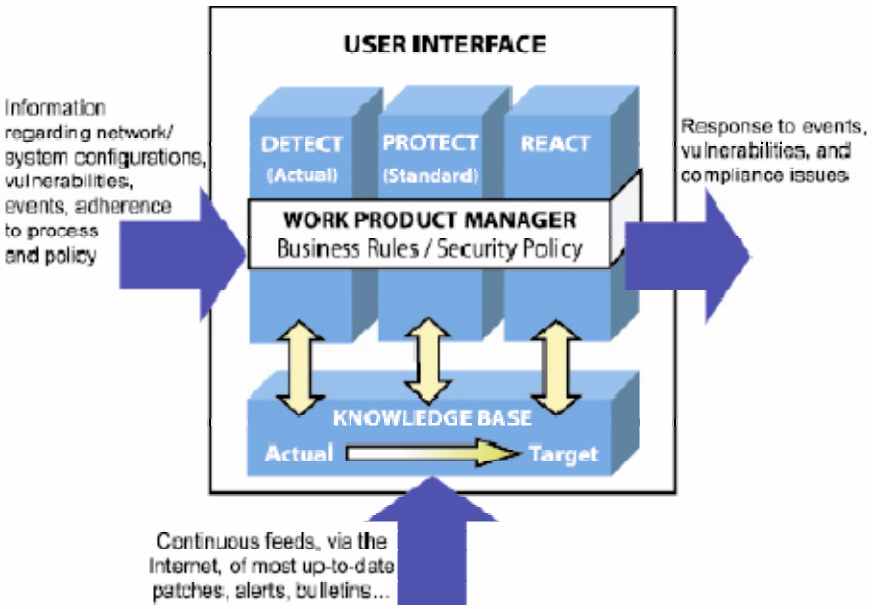


Figure 9. Xacta Web C&A and Xacta Commerce Trust Architecture [From 18)

Established in February 2000, Xacta Corporation employs approximately 120 professionals across the country with principal business offices in the Washington, D.C. and New York City areas. Formerly part of the e-solutions division of Telos Corporation, Xacta is now organized as a wholly owned subsidiary of Telos, one of the premier suppliers of network integration and systems development solutions to the Department of Defense and civilian agencies.

Xacta Corporation, a Telos company, develops, markets, and sells government-validated secure enterprise solutions to federal, state and local agencies, as well as to commercial customers. Xacta's offerings include enterprise IT security management solutions, enterprise security consulting services, enterprise messaging, secure wireless networking, and high assurance credentialing solutions

Telos Corporation has provided innovative IT solutions to the federal government for more than 30 years. The company provides systems integration and value added

reseller solutions to U.S. government customers. Telos and Xacta Corporation, its subsidiary for security solutions, have been ensuring that the government's most demanding and security-conscious organizations comply with existing and emerging information security mandates since 1989.

a. System Diagrams

Figure 11 a high level graphical representation of the overall architecture of the Xacta IA Manager Enterprise Edition. The Xacta IA Manager is an information security risk management application that consists of the Application Server, Detect Server, Publishing Server, and Graphical User Interface (GUI).

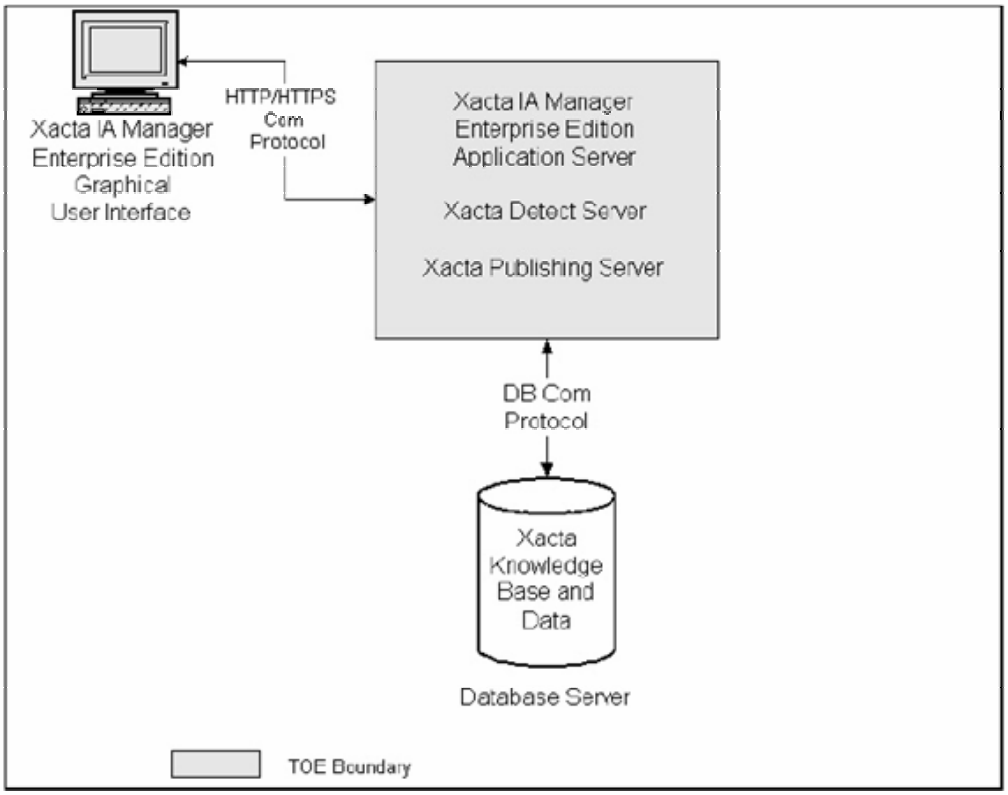


Figure 10. Xacta IA Manager Enterprise Edition Architecture Diagram [From 18)

Figure 12 is the Xacta IA Manager Process Enforcement Architecture. The Xacta IA Manager delivers an IT enterprise-level toolkit with secure management functionality. The IA Manager provides (1) an executive level reporting and management tool that displays key information, (2) process automation modules providing role-based

processes and audit trails and (3) content adapters that facilitate and coordinate the staff and their work with IA-related services such as enterprise management systems, resource applications, internet security software, security management software, databases, secure email and messaging.

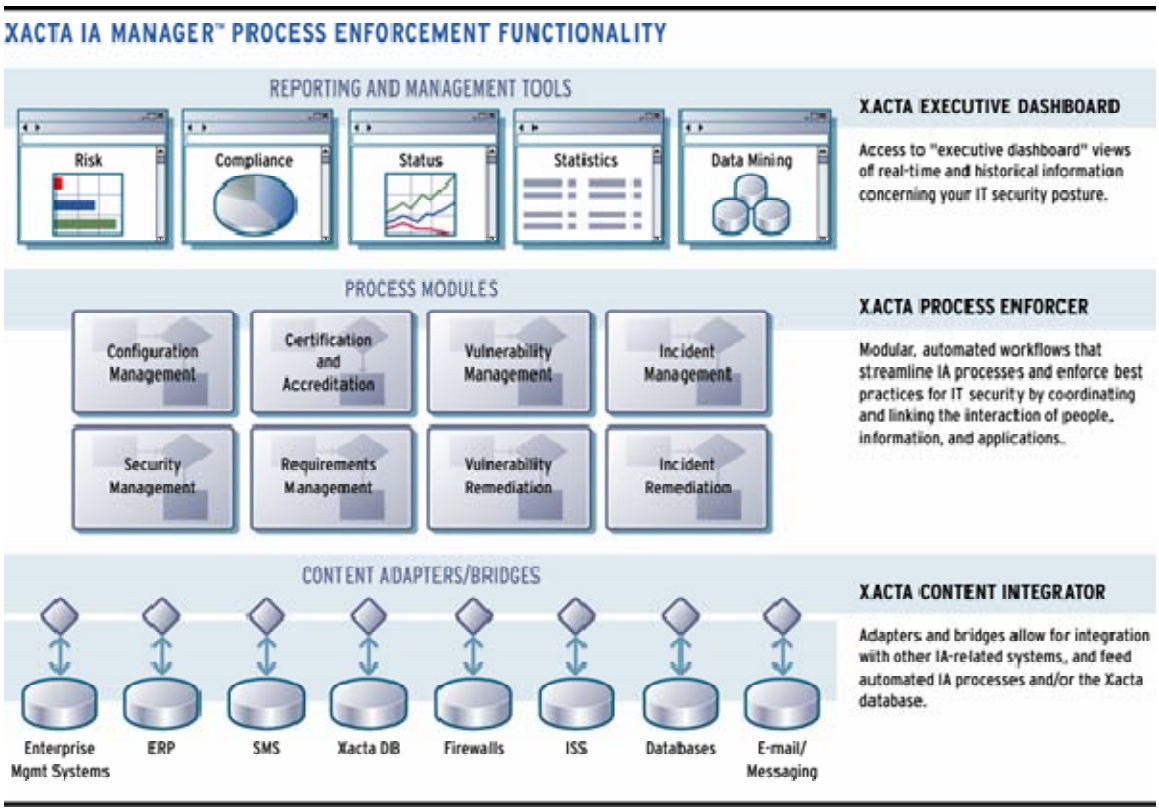


Figure 11. Xacta IA Manager Process Enforcement Architecture [From 18)

3. Functional Description

a. System Capabilities

The Xacta IA Manager helps the C&A team accelerate the organization's regulatory compliance and reporting. Some of the features and benefits that Xacta IA Manager provides (1) an essential capabilities necessary for the analysis of the organization's information security, (2) a Policy Locking and Enforcement feature where the C&A team can identify the organizations best security practices and implement these practices during the risk assessment and management process, (3) a checklist-based

security requirements which fill in the Security Requirements Traceability Matrix (SRTM) or related methods that need requirements mapping, (4) a Formal Test Plan that is generated dynamically designed to address system specific requirements and SRTM elements (5) an automated and streamlined presentation of the C&A process in accordance with federal and commercial regulatory requirements, including agency specific content and templates.

The Xacta IA Manager Upgrades provide additional C&A functionality to provide a more comprehensive solution in the secure management of the IT enterprise. Some of the key features of the Xacta IA Manager Upgrades are (1) a continuous collection of relevant configuration information on IT assets that enable the C&A team to regularly manage their risk and compliance posture to comply for constant C&A and risk assessment monitoring, (2) a method to capture Xacta's best business practices and assessment methodologies using the built-in wizard-driven templates that facilitate and clarifies C&A compliance assessment, (3) an automatic update feature on current vulnerabilities that provides continuous information on IT security threats and recommends real time corrective action with increased response time to counter possible threats, (4) an automatic information gathering utility that monitors critical shifts in the IT network environment, (5) a vulnerability and requirements based calculator that dynamically adjusts the IT enterprise risk and compliance posture.

The Xacta IA Manager Process Enforcement Upgrade delivers (1) a comprehensive, coordinated and automated risk management and remediation methodology for cross-enterprise deployment, (2) an automatic critical response system that triggers corrective action to address known vulnerabilities, inform essential personnel and log help desk trouble calls, (3) a software patch management system that automatically distributes and installs critical updates across the enterprise to ensure a current and updated security posture.

The Xacta IA Manager is supported by a unique collection of C&A technologies as shown in Figure 13.

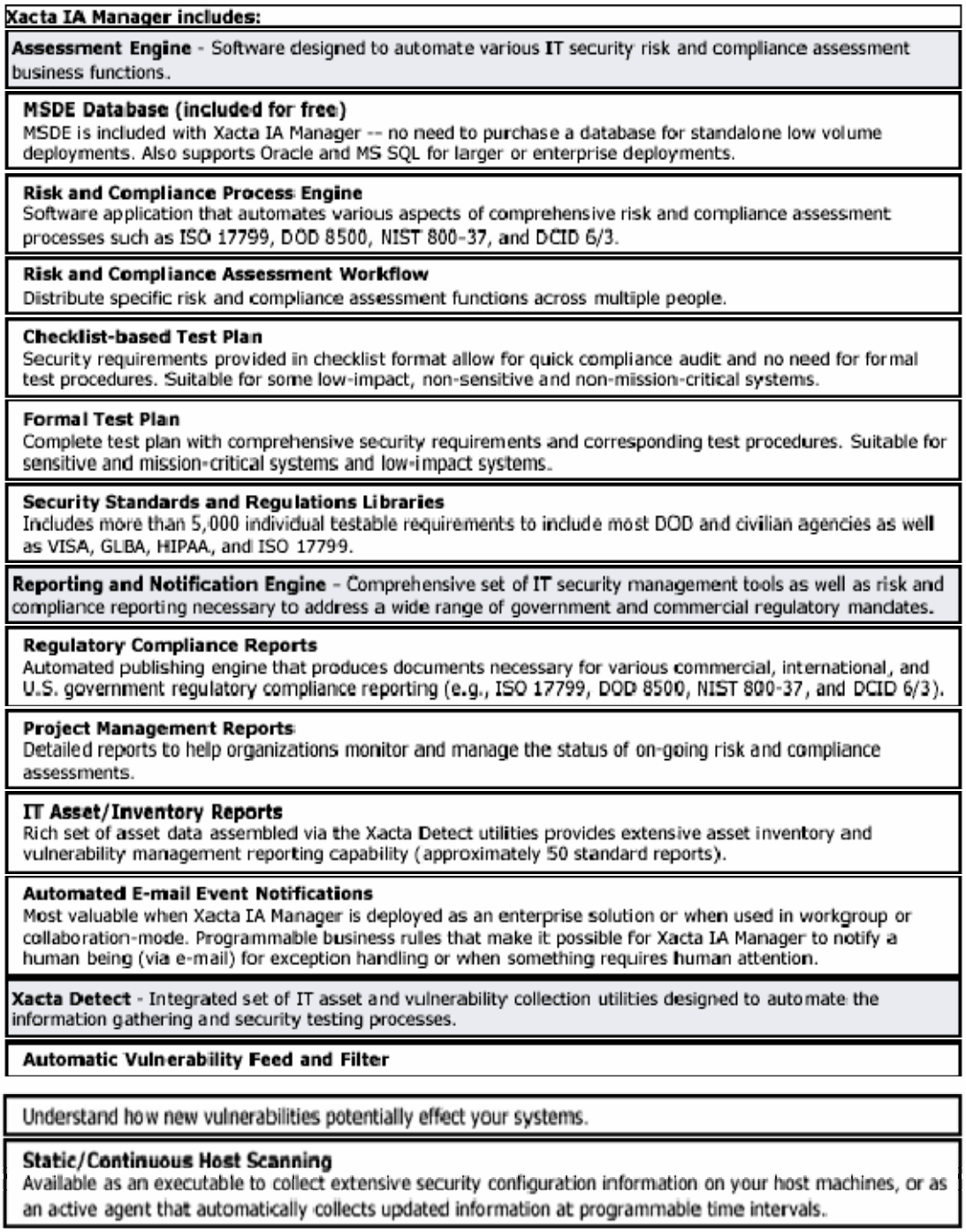


Figure 12. Summary of Xacta IA Manager features
[From 18]

Xacta IA Manager Upgrades	Continuous Assessment	Process Enforcement
Continuous Assessment Upgrade - Integrated utilities designed to automate certain risk and compliance assessment business functions.	✔	
Asset Information Readers (.xls, .xml) Import asset information automatically via spreadsheets and xml-formatted documents.	✔	
Vulnerability Scanner Java-based scanner with more than 3,000 plugins that are updated weekly.	✔	
Discovery Scanner NMAP-like functionality.	✔	
Asset Information Import Bridges Automatically import asset and vulnerability information from other systems such as SMS, Tivoli, ISS Scanner, and others.	✔	
Automatic Programmable Scanning Perform various collection and scanning functions to update risk and compliance posture at programmable intervals based on time or event triggers.	✔	
Automatic Recalculation of Risk and Compliance Updated asset information used to recalculate risk and compliance.	✔	
Automatic Event Notifications Notify users of important events regarding new devices, vulnerabilities and/or risk/compliance tolerances being exceeded.	✔	
Process Enforcer Upgrade – Continuous Assessment functionality plus integrated IT security process automation and integration technology designed to automate and accelerate security management functions, including vulnerability remediation.	✔	✔
Business Process Automation Synchronize security management business process across an entire organization.	✔	✔
Business Process Integration Components Interface with other business systems that support the security management process (e.g., help desk, enterprise management systems, etc.)	✔	✔
Business Process Designers Quickly modify and/or add automated business functions.	✔	✔
Business Process Monitor Real-time view of business process flows (status, bottlenecks, etc.)	✔	✔

Figure 13. Summary of features for Xacta IA Manager Upgrade and Process Enforcer Upgrade

[From 18]

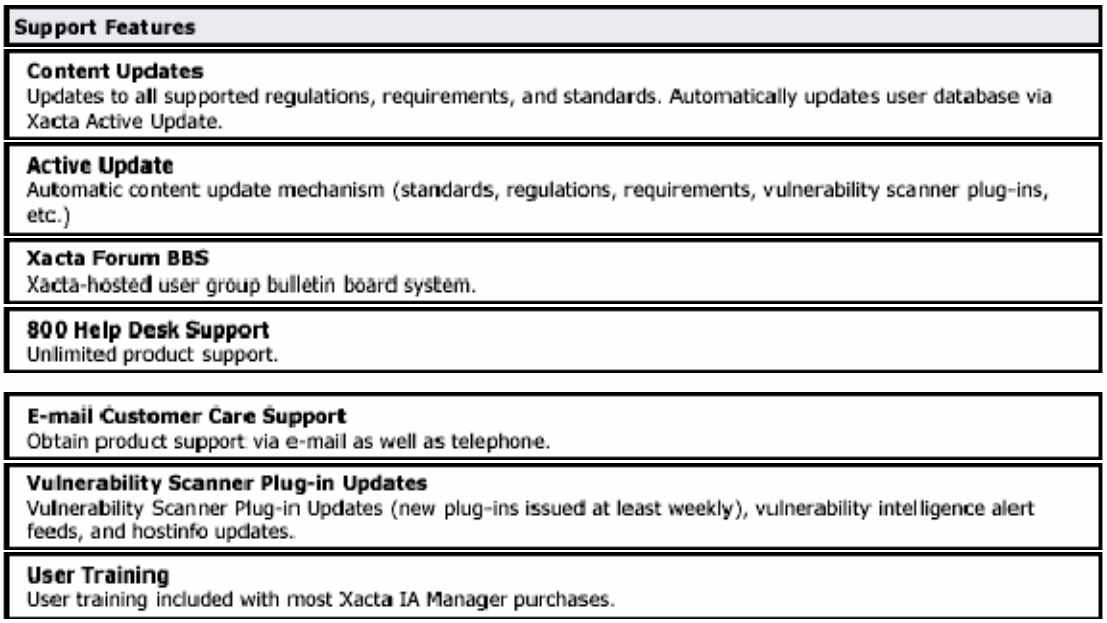


Figure 14. Summary of features for Xacta IA Manager Support Features [From 18]

b. System Classification

The intent of this section is purely informational and not marketing. The purpose of the data is to inform potential C&A users that the Xacta tool is certified under the Common Criteria. This information is not intended to persuade but inform potential C&A users of the facts related to the certification of the Xacta automated C&A tool.

In accordance with the Common Criteria (CC) for Information Technology Security Evaluation, Version 2.2, January 2004 (CCV2.2) ISO/IEC 15408 and Common Methodology for Information Technology Security Evaluation, Version 2.2, Evaluation Methodology, January 2004 (CEMV2.2), which is now the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme for Information Technology Security, this system is has been certified as an Evaluation Assurance Level 2 (EAL2). This system has been evaluated at CygnaCom Solutions, an accredited testing laboratory. The Xacta IA Manager's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with NIAP CC Evaluation and Validation Scheme and the

conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence presented.

The Common Criteria are standards for evaluating security software against vendor claims or user requirements. Evaluation is done by approved private laboratories and is recognized by multiple nations. The program is overseen in the United States by the NIAP, a joint effort between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Common Criteria certification for security products is required by the Defense Department, and on national security systems in the federal government.

c. Classification and Sensitivity of Data Processed

Information that is stored, processed, and transmitted on, through and/or from Xacta IA Manager is considered Sensitive But Unclassified and should be marked as For Official Use Only (FOUO). All FOUO data is protected by measures appropriate for unclassified system high operations. Controls for need-to-know information are an element of the protective mechanisms placed on Xacta IA Manager. All system administration information contained in Xacta IA Manager Application Server is under the cognizance of the Xacta built-in Master Administrator..

d. System User Description and Clearance Levels

The Xacta IA Manager Enterprise Edition has a web based graphical user interface through which all Xacta IA Manager Enterprise Edition functions are managed. It supports four roles, built-in master administrator, administrator, executive and user. A primary function of the application administrator is to create security assessment "projects", create "user" accounts for persons who will work on those projects, and assign the users to the appropriate projects (based on a project role). As a way of managing or grouping accounts and projects, the administrator has the option to segregate these accounts and projects objects into "folders". Security policy settings for usernames and passwords are established through the GUI. Also, administrators use the GUI to enable or disable audit logging and to review and archive the audit trail. The Built-in Master Administrator and Administrator accounts use the administrator Interface.

Normal user login results in the presentation of a list of projects to which a user has been assigned. The user's access to projects is based on their assignment to

specific project roles within a project. (More than one user may be assigned to any particular role within a project.) The primary functions a user executes within the application include the following tasks:

- Requirements & Definition: the user describes the security boundary of a particular automated information system (AIS) and identifies the security requirements that it will be evaluated against

- Inventory & System Information: the user identifies all components within the system boundary and provides other detailed project information

- Vulnerability Assessment & Testing: the user completes checklists, prepares test plan documentation, and enters test results

- Analysis and Reporting: the user performs in-depth analysis of risks identified for the system and completes required deliverable documentation.

Each of these tasks is executed through a series of process steps. Based on the particular role to which a user has been assigned, not all of these tasks will be visible (or accessible). The arrangement of "Tasks" and "Process Steps" within any project is customizable and may vary from one project to the next. (Customers may also define agency-specific workflows and disseminate these in the form of a project template.) Both the Executive and User accounts use the User Interface.

e. Life Cycle of the System

Xacta IA Manager is in the implementation and maintenance stage of its life cycle. It is an information risk management application project funded by the Telos Corporation. Its purpose is to streamline the organization's C&A and continuous risk assessment, automate security business processes across the enterprise, provide full automation support for numerous federal, DoD and civilian compliance standards, and perform comprehensive IT management. It utilizes patent pending technologies that enable the creation and maintenance of a continuous sequence of automated IT security processes configured to the enterprise specific requirements.

The configuration and operation of Xacta IA Manager conforms to the life cycle design and execution strategy required for all federal, DoD and civilian owned information systems.

f. Minimum System Requirements

The minimum system requirements for Xacta IA Manager include products formerly known as Xacta Web C&A and Xacta Commerce Trust.

Assessment Engine - Single Server Deployment

The single-server installation is recommended for small networks or for a standalone system typically employed by those performing static compliance/risk assessments. The following are the minimum requirements for a single-server installation: [From 18]

Server/Desktop/Laptop

- Pentium 4 (2 GHz Processor)
- 1 GB RAM
- 40 GB Hard Drive
- MS Office 2000, MS Office XP, MS Office 2003
- MSDE or MS SQL Server 2000 (Service Pack 3 or above) or Oracle 8i/9i/10g
- MS Windows 2000 Server/Pro or MS Windows XP Pro or MS Windows 2003 Server

Assessment Engine - Standard Network Deployment

The standard multi-server installation is recommended for medium-sized enterprises or regional installations that are part of a larger distributed installation. The recommended configuration for a standard network deployment consists of two server-class machines: an application server and a database/publishing server. The following are the minimum requirements for a standard network installation:

Application Server

- Pentium 4 (1.8 GHz Processor)
- 2 GB RAM
- 40 GB Hard Drive
- MS Windows 2000 Server or MS Windows 2003 Server

Database - Publishing Server

- Pentium 4 (1.8 GHz Processor)
- 2 GB RAM
- 60 GB Hard Drive
- MS Office 2000, MS Office XP, MS Office 2003

- MS SQL Server 2000 (Service Pack 3 or above. When using SQL Server, approximately 120 GB of database storage space will need to be available) or Oracle 8i/9i/10g
- MS Windows 2000 Server or MS Windows 2003 Server

Assessment Engine - High Volume Network Deployment

The high-volume multi-server installation is recommended for enterprises that have a large number of projects and wish to maintain centralized control over the data. The recommended configuration for a high-volume network deployment consists of three server-class machines: an application server, a database server, and a publishing server. The following are the minimum system requirements for a high-volume network installation: [From 18]

Application Server

- Pentium 4 (2.4 GHz Processor)
- 2 GB RAM
- 40 GB Hard Drive
- MS Windows 2000 Server or MS Windows 2003 Server

Database Server

- Pentium 4 (2.4 GHz Processor)
- 2 GB RAM
- 120 GB Hard Drive
- MS SQL Server 2000 (Service Pack 3 or above; when using SQL Server approximately 120 GB of database storage space will need to be available) or Oracle 8i/9i/10g
- MS Windows 2000 Server or MS Windows 2003 Server

Publishing Server

- Pentium 4 (1.8 GHz Processor)
- 1 GB RAM
- 40 GB Hard Drive
- MS Office 2000, MS Office XP, MS Office 2003
- MS Windows 2000 Server or MS Windows 2003 Server

Microsoft (MS) Office Installation

The Xacta Publisher component requires all MS Word files and libraries to be installed.

The minimum system requirements for Xacta IA Manager Continuous Assessment Upgrade include the Xacta Detect Server and Client. The Xacta Detect Server is a network and vulnerability scan engine. It is included in the Professional Edition as a standalone client-server scanner. In the Enterprise and Process Enforcement Editions, the core Assessment Engine controls the Xacta Detect Server in Continuous Assessment mode. Multiple Xacta Detect Servers can be installed to accommodate segmented or distributed networks. [From 18]

- Xacta Detect Server is supported on MS Windows 2000 Server/Pro and MS Windows XP Pro.

- The Xacta Detect Client is a networked GUI client that can be installed on any MS Windows platform.

Access Requirements:

- Microsoft Internet Explorer 6 or Netscape Navigator 7
- TCP/IP connection to the application
- Access to a printer
- Adobe Acrobat Reader 5.0 and above

Recommended Installation and Administration Skills:

- MS Windows 2000, XP and/or 2003 administration skills
- MS SQL Server or Oracle database administration knowledge
- General Internet and TCP/IP networking knowledge

The minimum system requirements for Xacta IA Manager Process Enforcer Upgrade are: [From 18]

Server Platforms:

Windows:

- Pentium 4 (1.8 GHz Processor)
- 2 GB RAM
- 40 GB Hard Drive
- MS Windows 2000 Server/Pro or MS Windows XP Pro
- 240 MB disk space for a full installation of Process Enforcer
- Minimum 500 MB temporary space free on the drive to be used for installation
- DBMS: MS SQL Server 2000 SP3 or Oracle 8i or 9i.

UNIX

- HP-UX 11.0 C class or better (PA RISC 2) (400 MHz Processor) or Sun Solaris 2.8
- 2 GB RAM
- 40 GB Hard Drive
- 240 MB disk space for a full installation of Process Enforcer
- Minimum 500 MB temporary space free on the drive to be used for installation
- DBMS: MS SQL Server 2000 SP3 or Oracle 8i or 9i.

Client Platforms

Process Enforcer Design Console:

- Pentium 4 (600 MHz Processor)
- 512 MB RAM
- MS Windows 2000 Server/Pro or MS Windows XP Pro

Task Manager and Report Tool:

- Pentium 4 (600 MHz Processor)
- 512 MB RAM
- MS Windows 2000 Server/Pro or MS Windows XP Pro

The minimum system requirements for Xacta IA Distribution Manager are: [From 18]

- Pentium 4 (2 GHz Processor)
- 1 GB RAM
- 60 GB Hard Drive
- MS Windows 2000 Server, MS Windows Server 2003
- MS SQL Server 2000 SP3 or Oracle 8i/9i/10g Server

The following are the network and client minimum system requirements needed to access and use the Process Enforcer Task Manager, Process Enforcer Report Tool and/or Distribution Manager:

- Microsoft Internet Explorer 6 or Netscape Navigator 7
- TCP/IP connection to the Xacta Process Enforcer application server
- TCP/IP connection to the Xacta Distribution Manager application server
- TCP/IP connection to the Xacta IA Manager Assessment Engine application server

The following are the recommended installation and administration skills for Process Enforcer and Distribution Manager:

- MS Windows 2000, XP and/or 2003 server administration skills
- HP-UX 11.0 administration skills or Sun Solaris 2.8 administration skills (Process Enforcer only)
- MS SQL Server or Oracle database administration knowledge
- General Internet and TCP/IP networking knowledge

4. Xacta Graphic User interface (GUI)

a. Using the Application

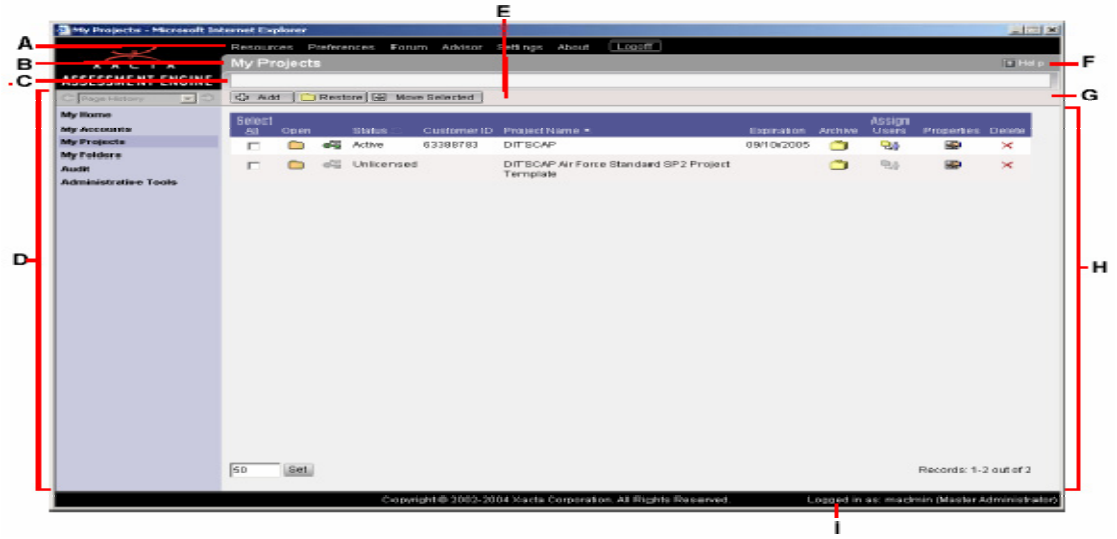


Figure 15. Application Interface
[From 18]

1. Item A, the Menu Bar is located at the top of the screen and contains the following menus and links:

- The Resources menu opens a window containing links to the Assessment Engine Reference Manual (in .pdf format) and to the Adobe website where Adobe Acrobat Reader can be downloaded.
- The Preferences menu opens a window containing options to set user preferences.
- The Settings menu, visible only to a master administrator, opens a window from which all system settings can be accessed.
- The About menu opens a window containing information about the version number of the application, as well as the license agreement and credits.
- The Logoff link is used to log out of the application.

2. Item B, the Page Title is located below the Menu Bar and displays the title of the page you are currently viewing.

3. Item C, the Message Area is located directly below the Page Title area and dynamically displays informative messages based on your actions; such as Save confirmation, errors, status information, and tips.

4. Item D, the Left Navigation Bar is located on the left side of the screen and is used to navigate through the application.

5. Item E, the Action Bar is located below the Message Area and contains action buttons for the page you are viewing.

6. Item F, a Help button is located to the right of the Page Title area. This help is context-sensitive and displays help pertaining to the current page. If you need additional assistance, you can view the entire application reference manual in .pdf format. The Assessment Engine Reference Manual is found under the Resources menu at the top of the screen.

7. Item G, when working on a process step, the Previous Step and Next Step buttons are displayed on the Action Bar (they are not displayed in the diagram because a process step is not open). These buttons are used to quickly move to the next process step or return to the previous process step.

8. Item H, the Content Area occupies the majority of the application screen and contains all the input fields and data relevant to the current page.

9. Item I, the Status Bar displays the account name and type of account currently logged in the lower-right corner of the screen.

b. Preparing Assessment

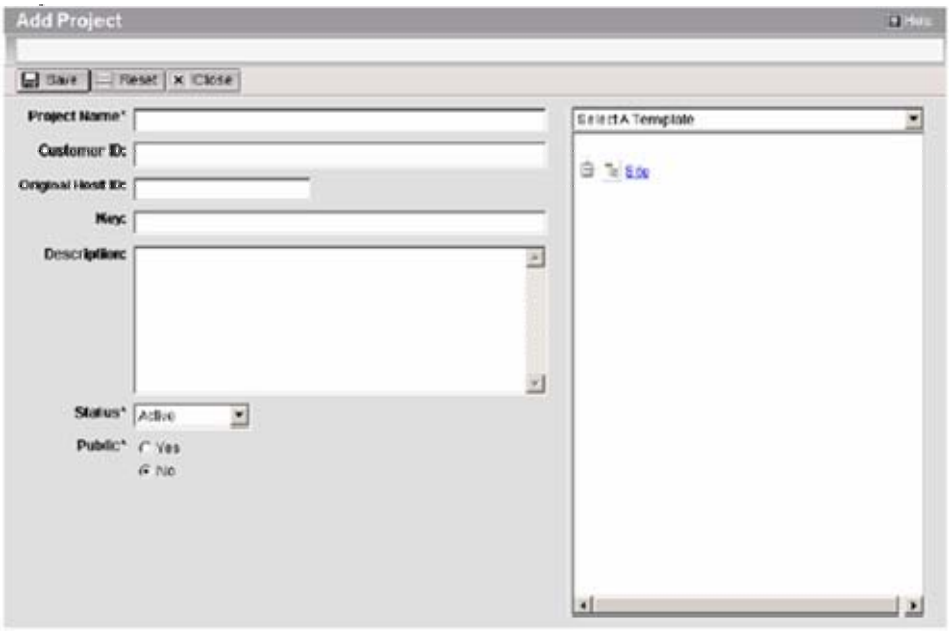


Figure 16. Adding Project
[From 18]

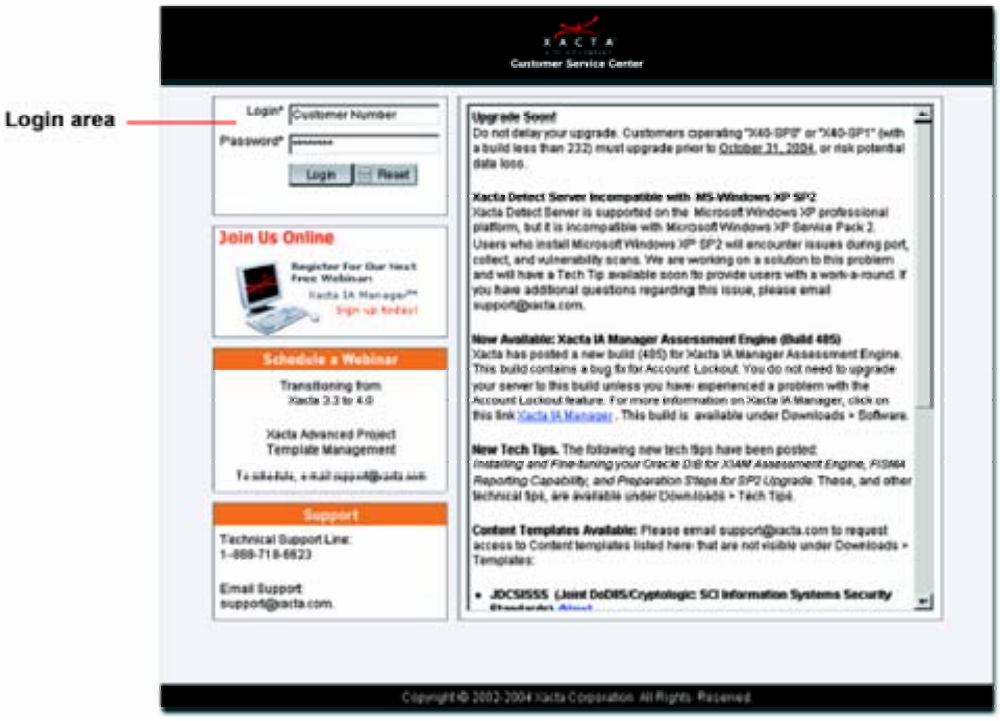


Figure 17. Logging Customer Service Center
[From 18]

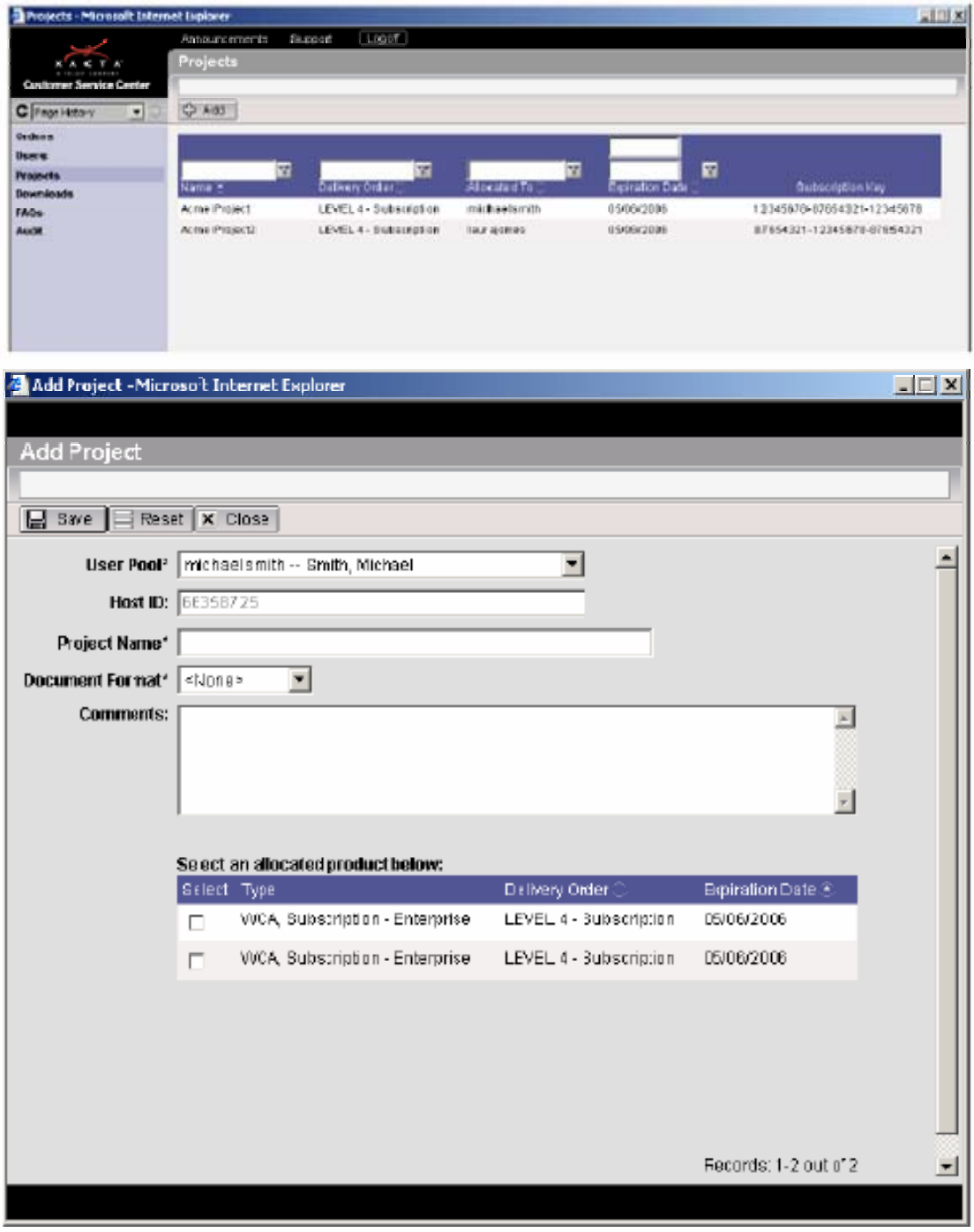


Figure 18. Allocate Products to Users
[From 18]

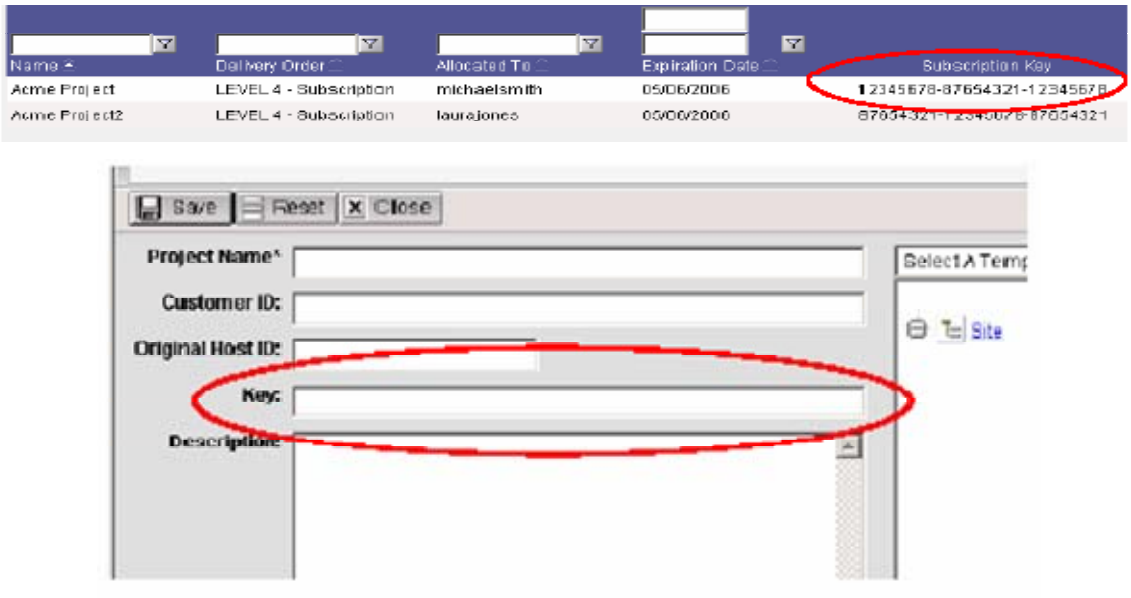


Figure 19. Entering Subscription Key to Assessment Engine
[From 18]

Figure 20. Selecting Template
[From 18]

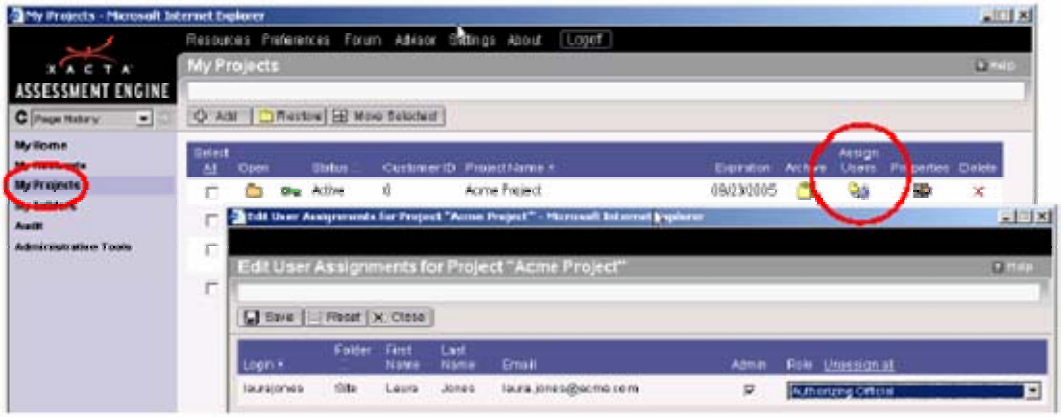


Figure 21. Creating Folder Level Accounts
[From 18]

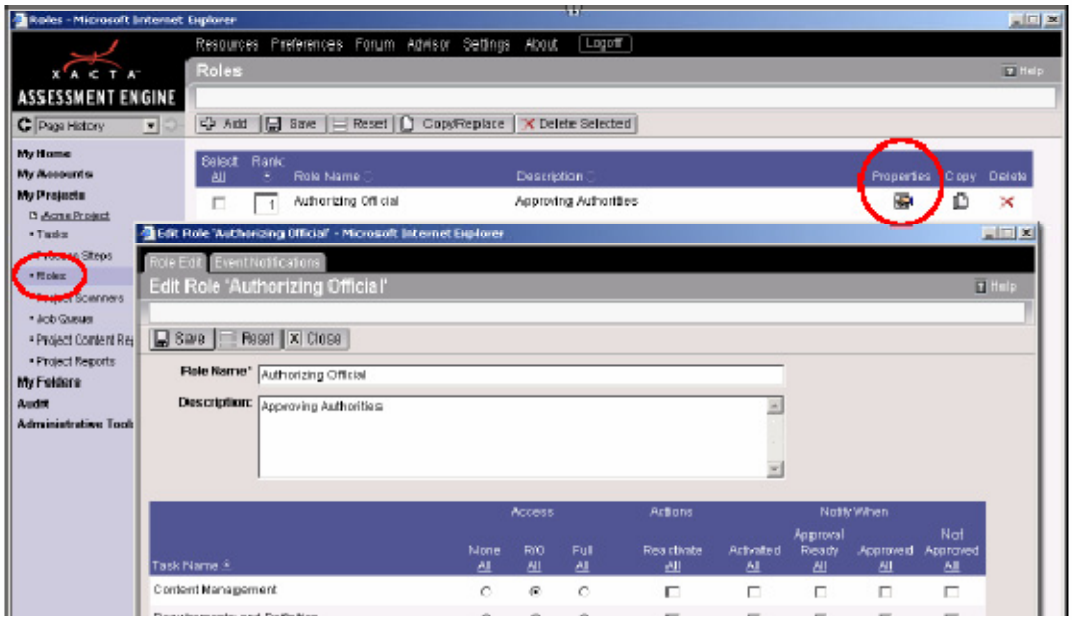
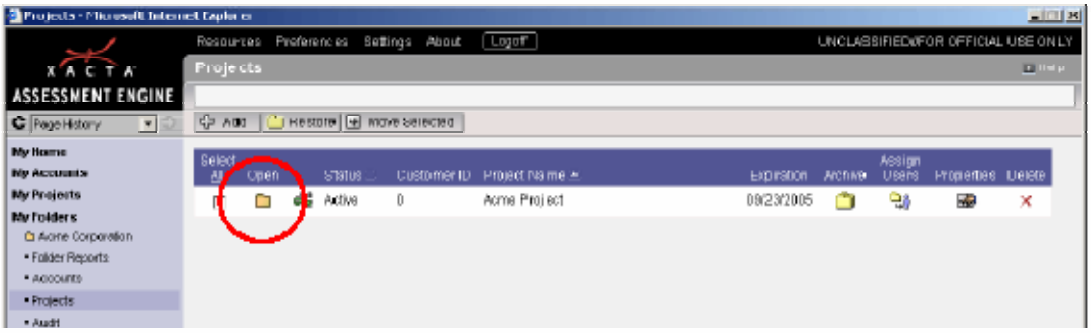


Figure 22. Creating Roles
[From 18]

c. Performing Assessment



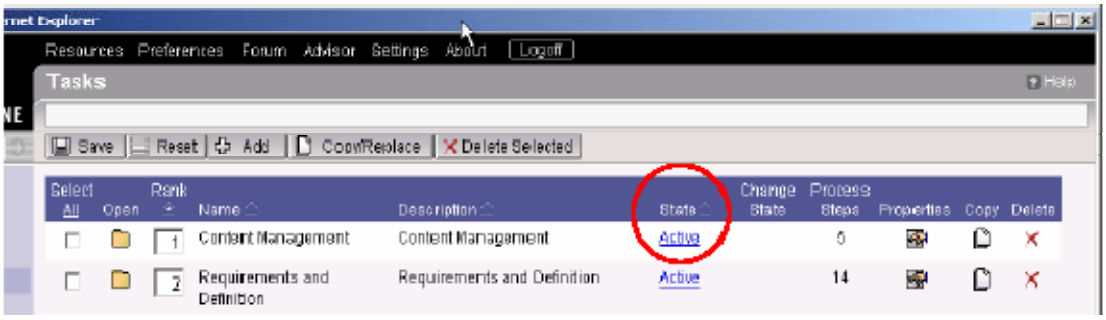


Figure 23. Task Page and Task State
[From 18]

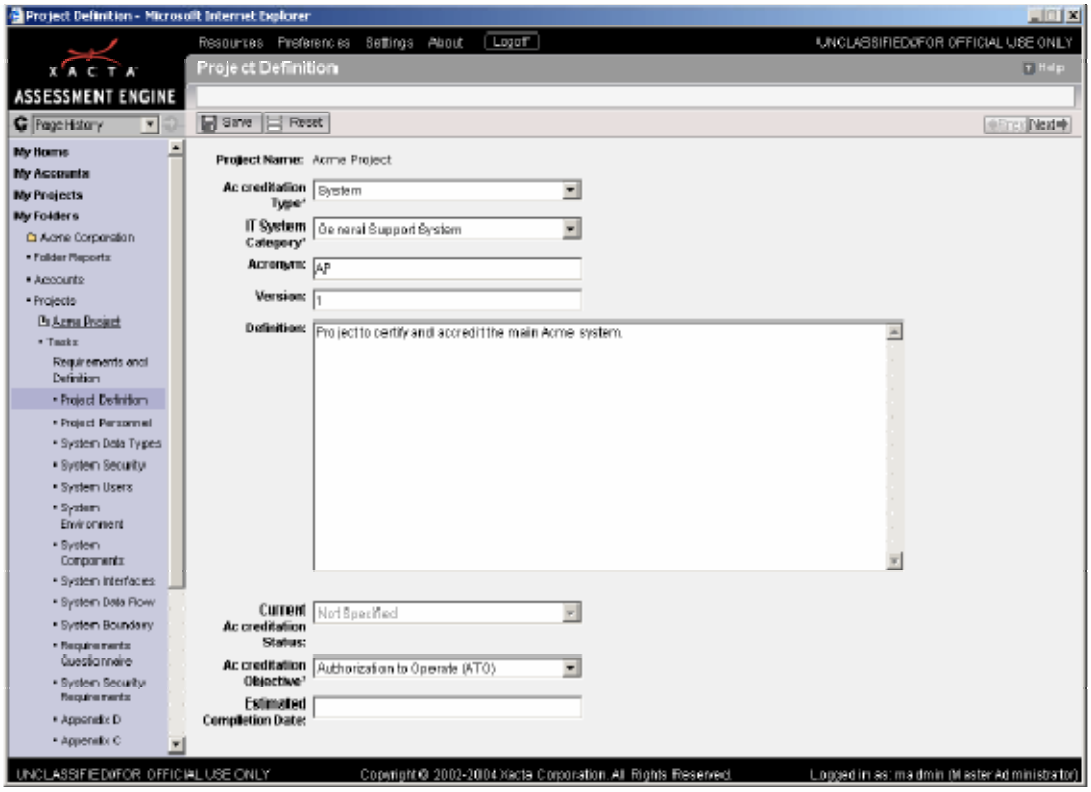


Figure 24. Project Definition
[From 18]

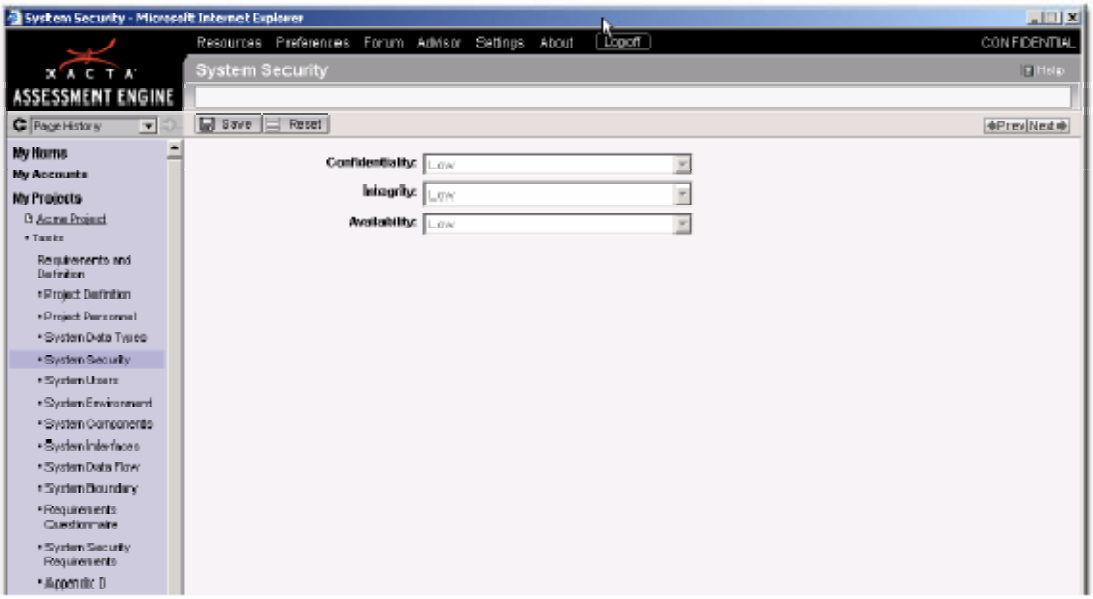


Figure 25. System Security
[From 18]

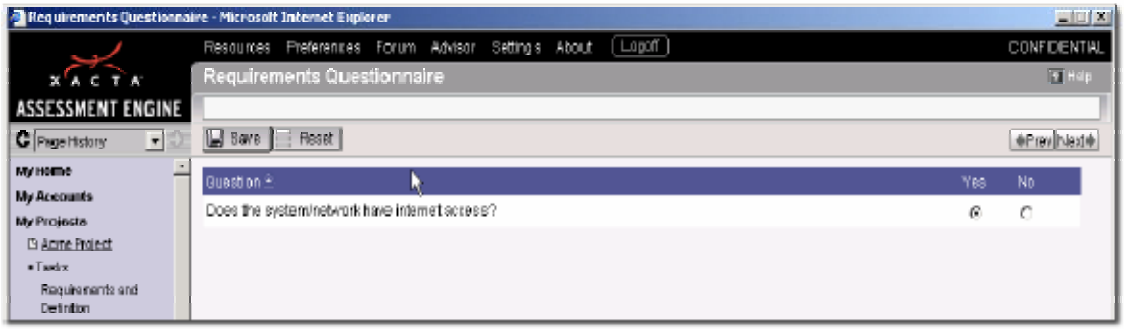


Figure 26. Requirements Questionnaire
[From 18]

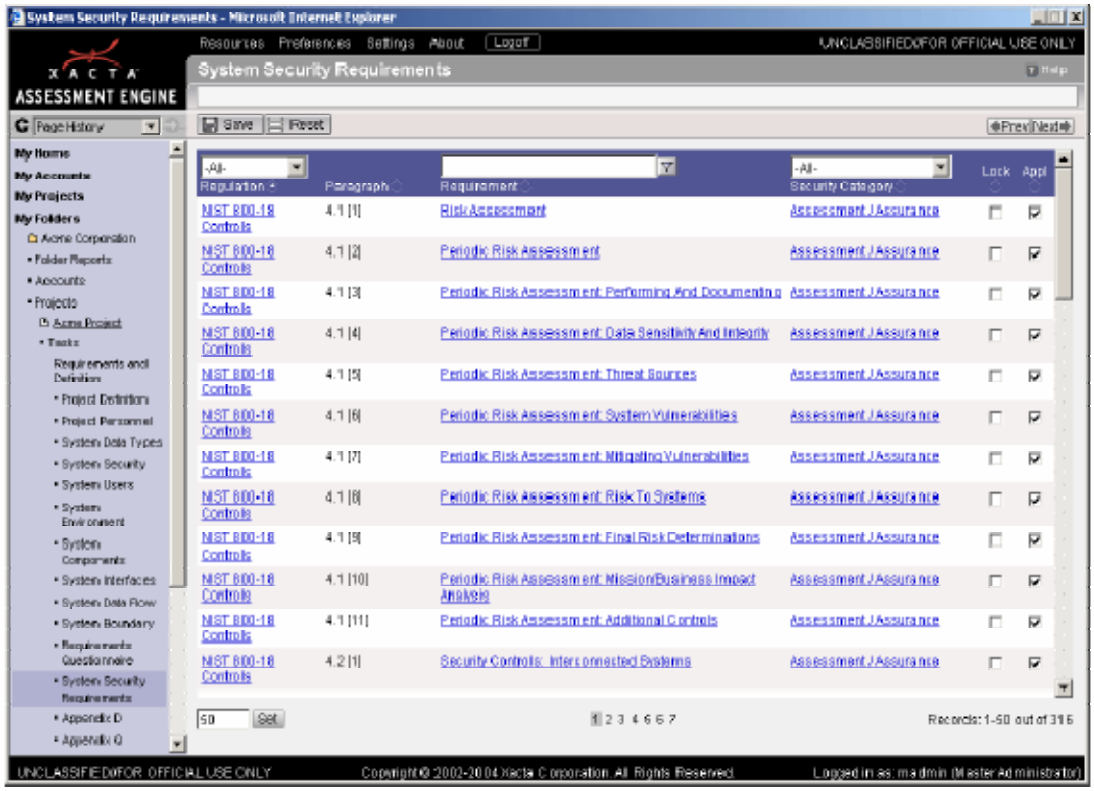


Figure 27. System Security Requirements
[From 18]

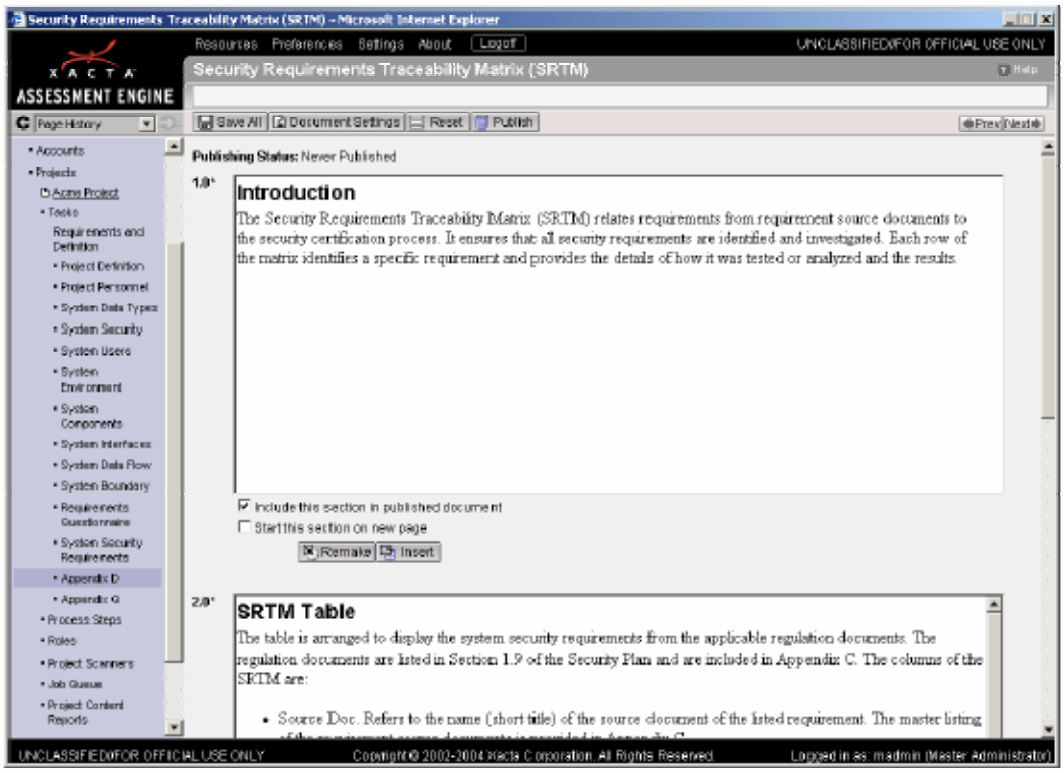


Figure 28. Security Requirements Traceability Matrix
[From 18]

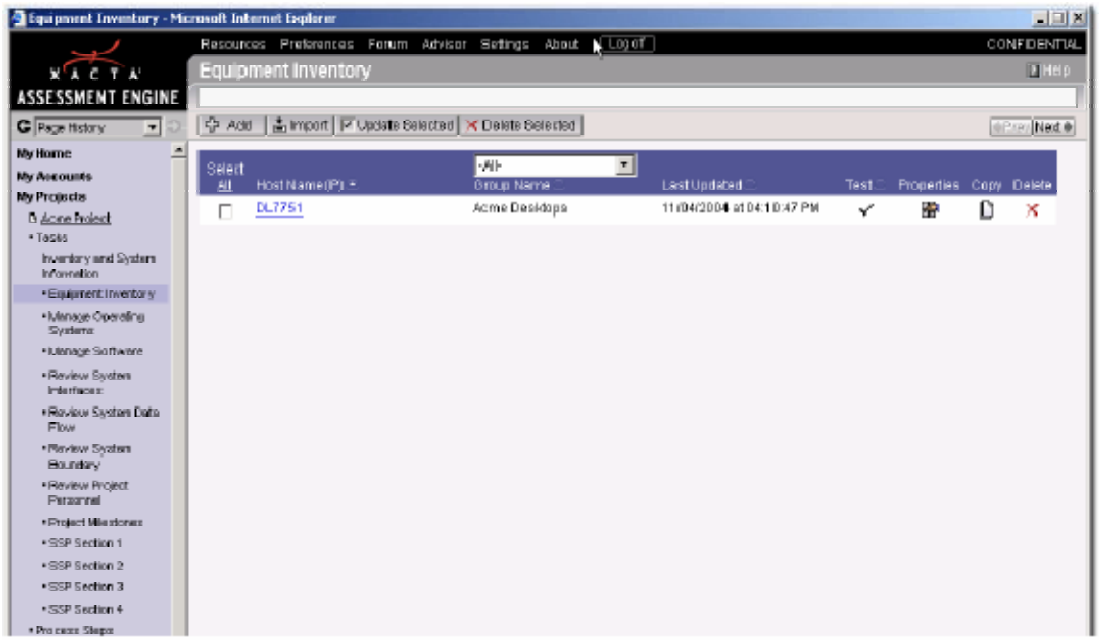


Figure 29. Equipment Inventory
[From 18]

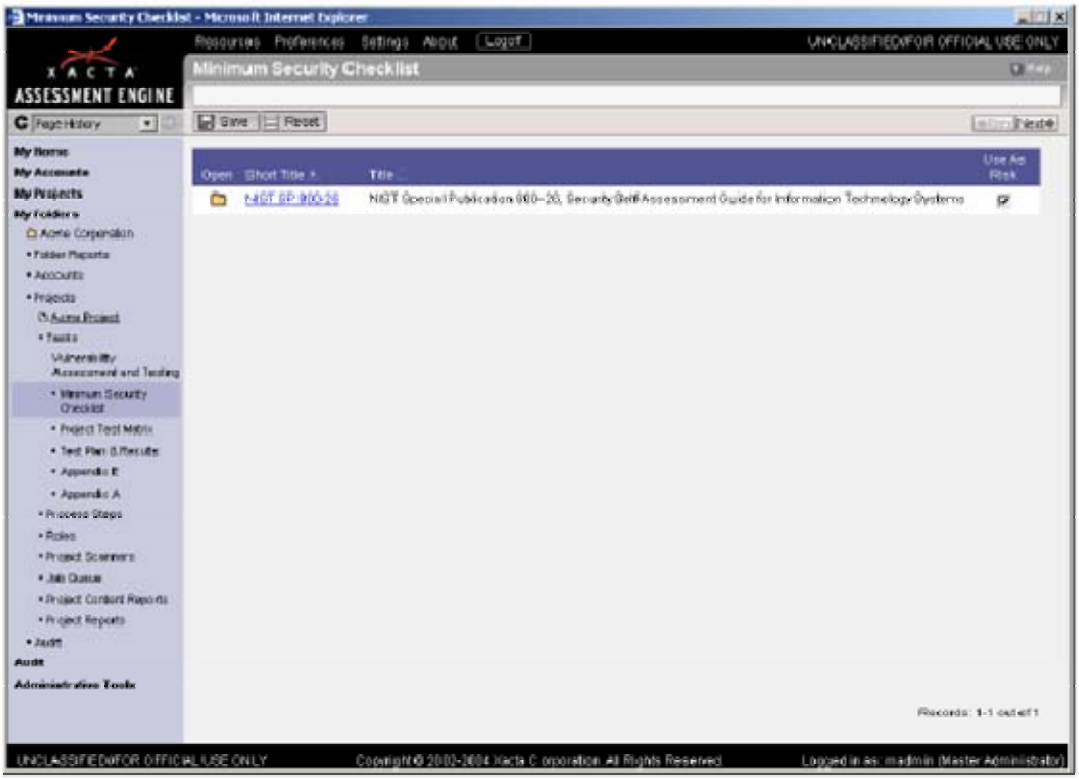


Figure 30. Minimum Security Checklist
[From 18]

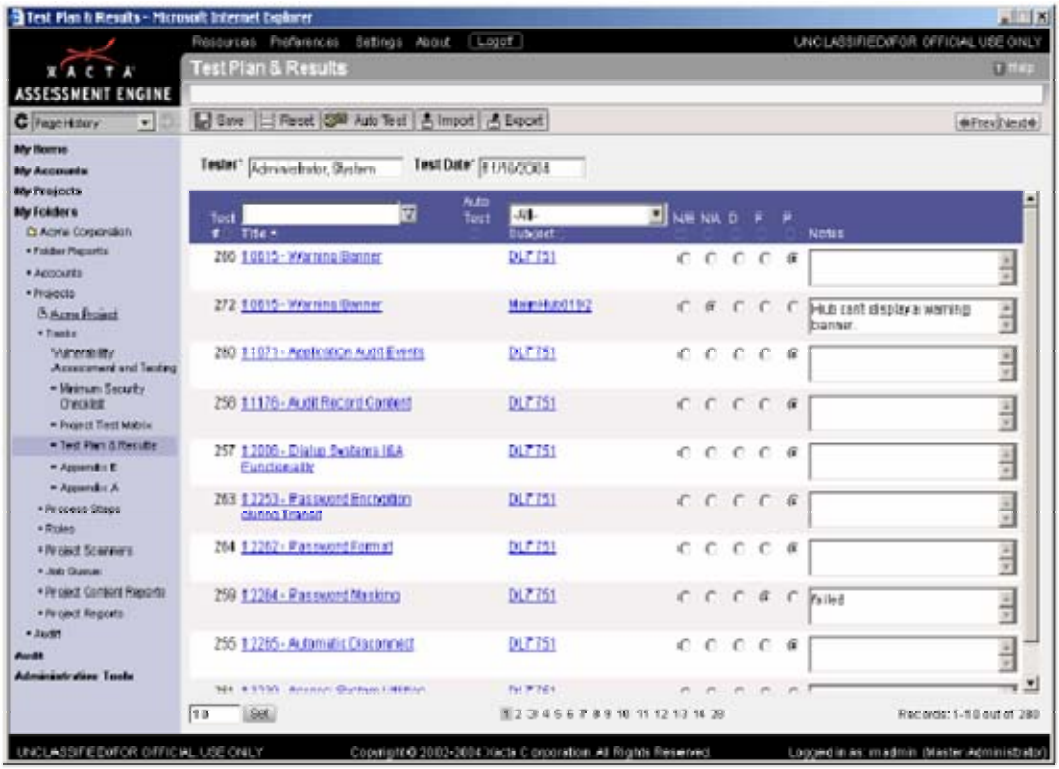


Figure 31. Test Plan and Results
[From 18]

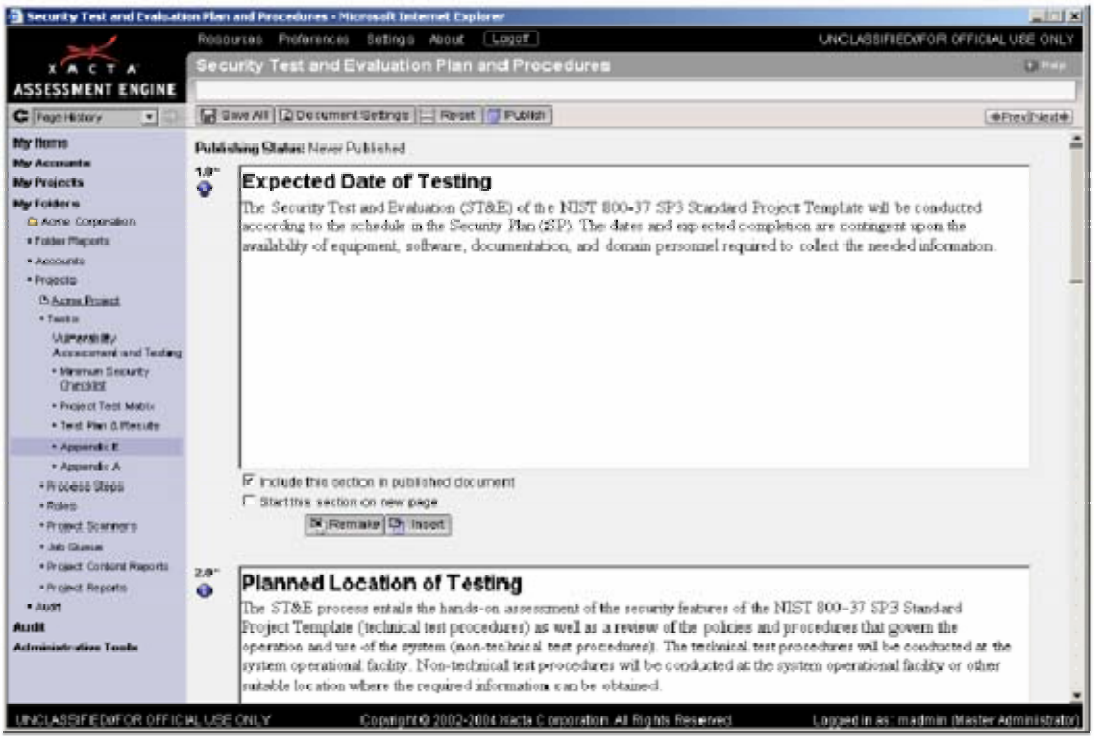


Figure 32. Security Test and Evaluation
[From 18]

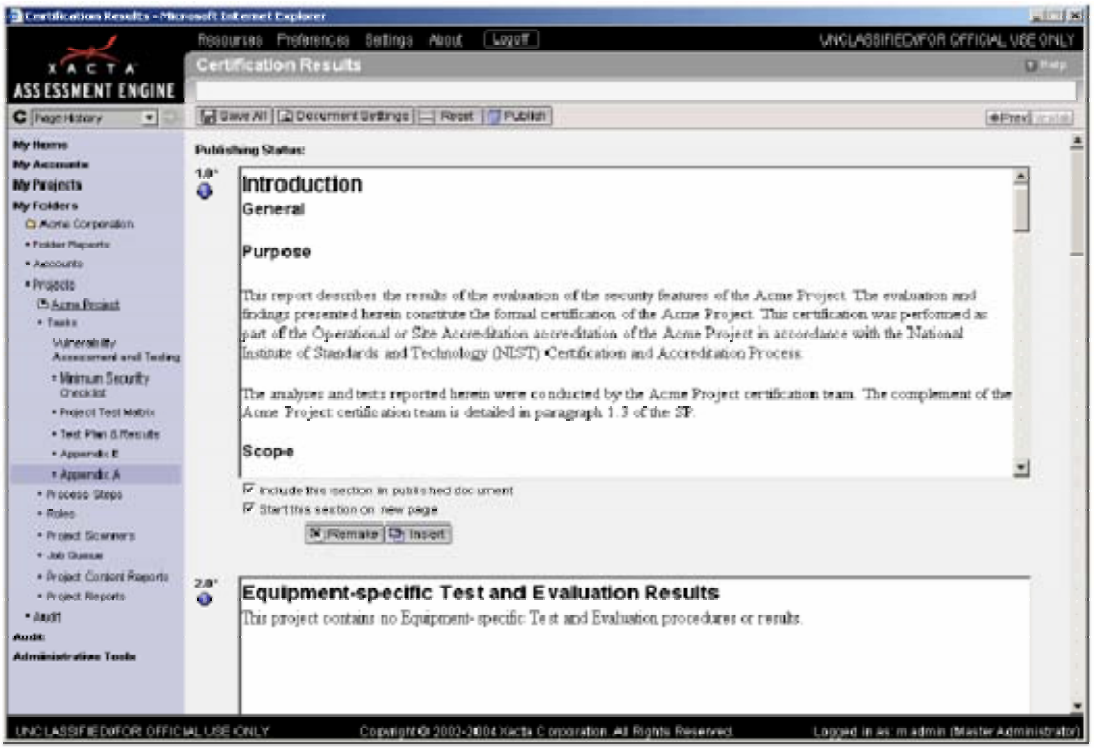


Figure 33. Certification Results
[From 18]

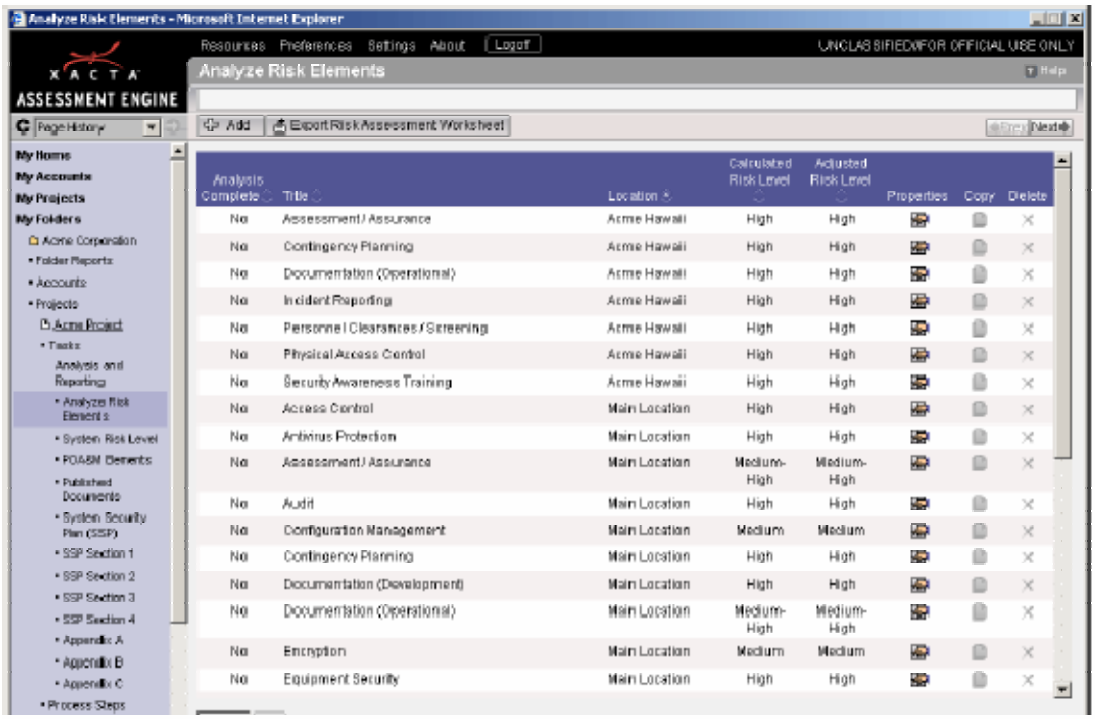


Figure 34. Analysis of Risk Elements
[From 18]

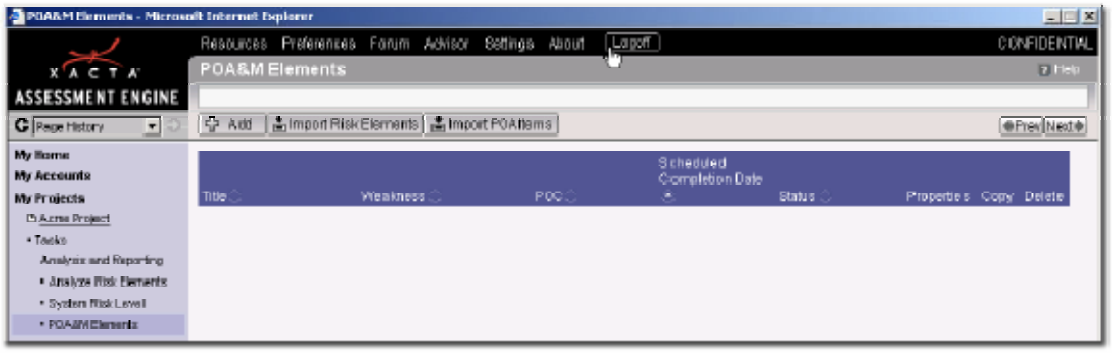


Figure 35. Plan of Action and Milestones (POA&M) Elements
[From 18]

d. Reports

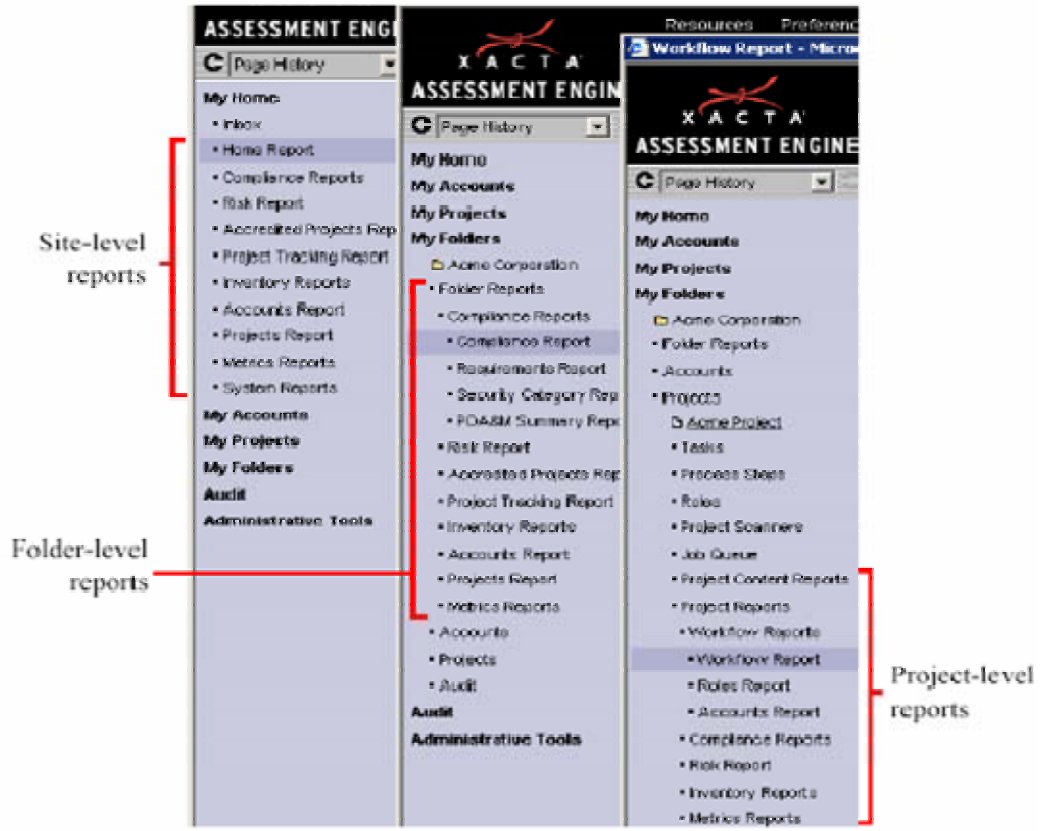


Figure 36. Reports Overview
[From 18]

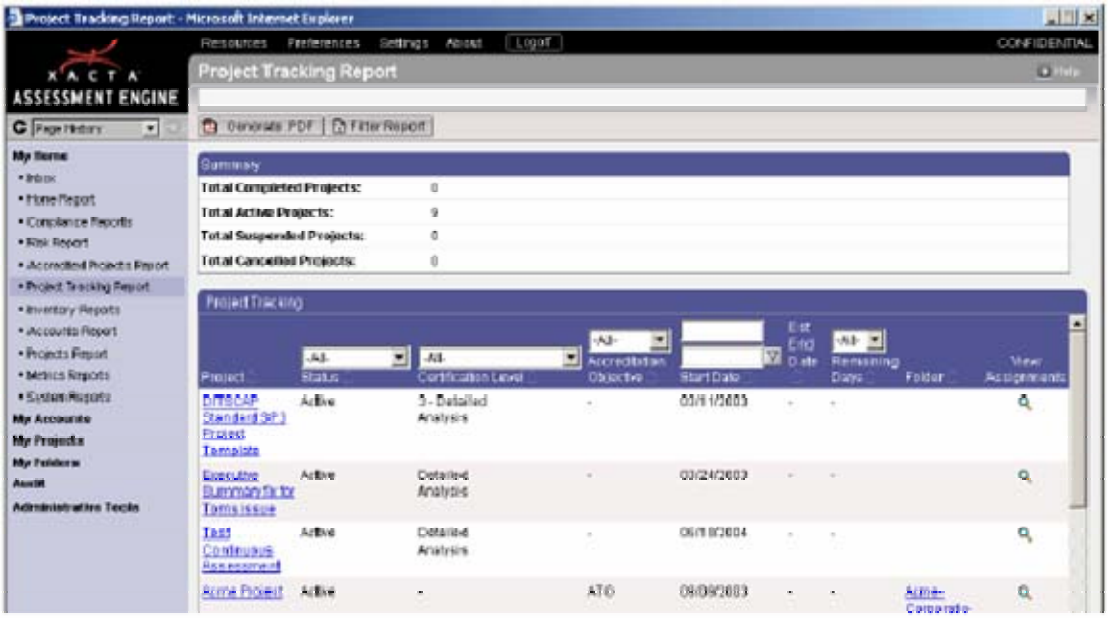


Figure 37. Project Tracking Report
[From 18]

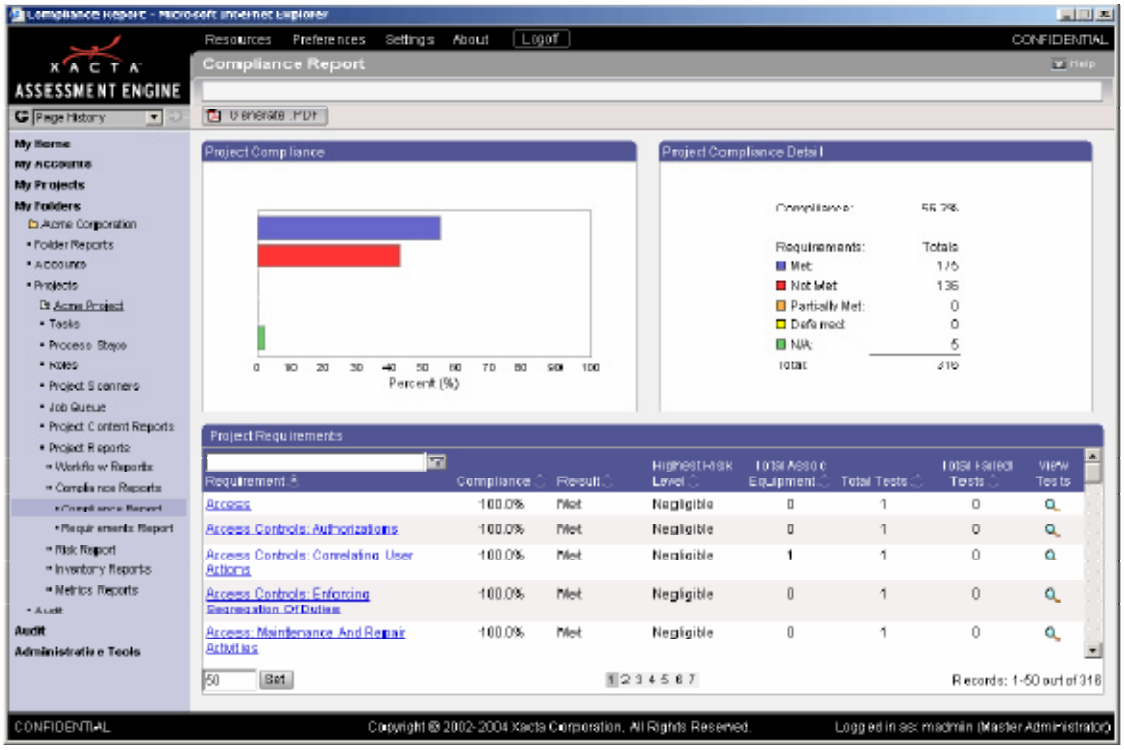


Figure 38. Compliance Report
[From 18]

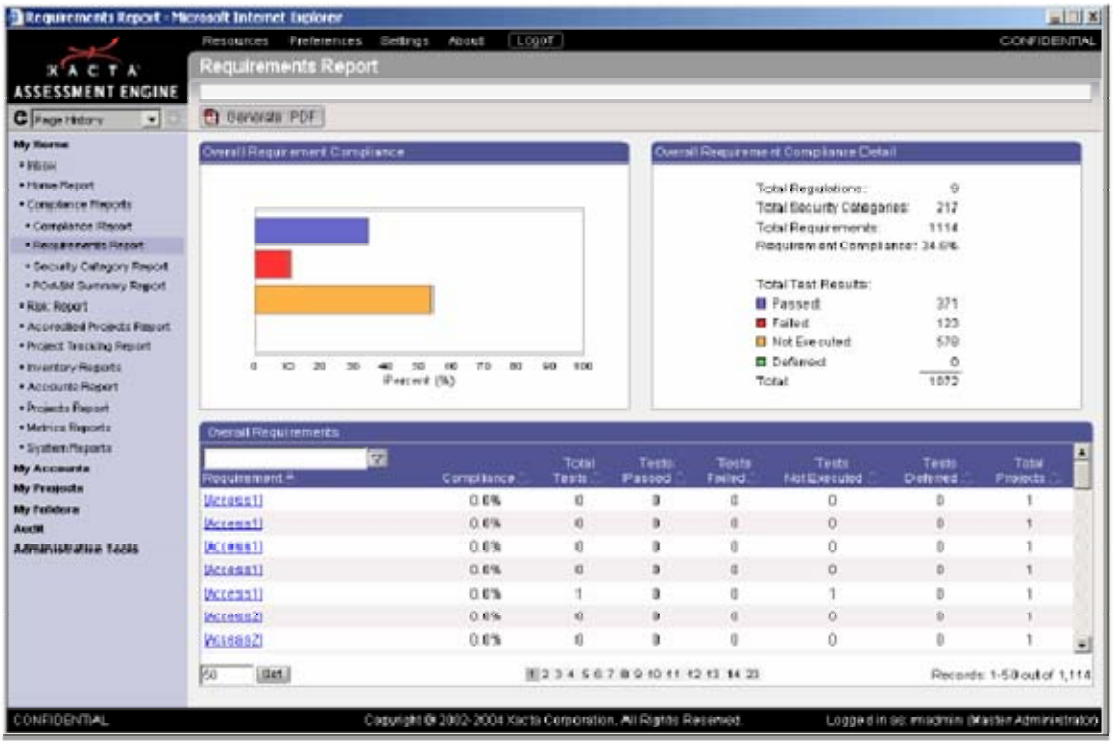


Figure 39. Requirements Report
[From 18]

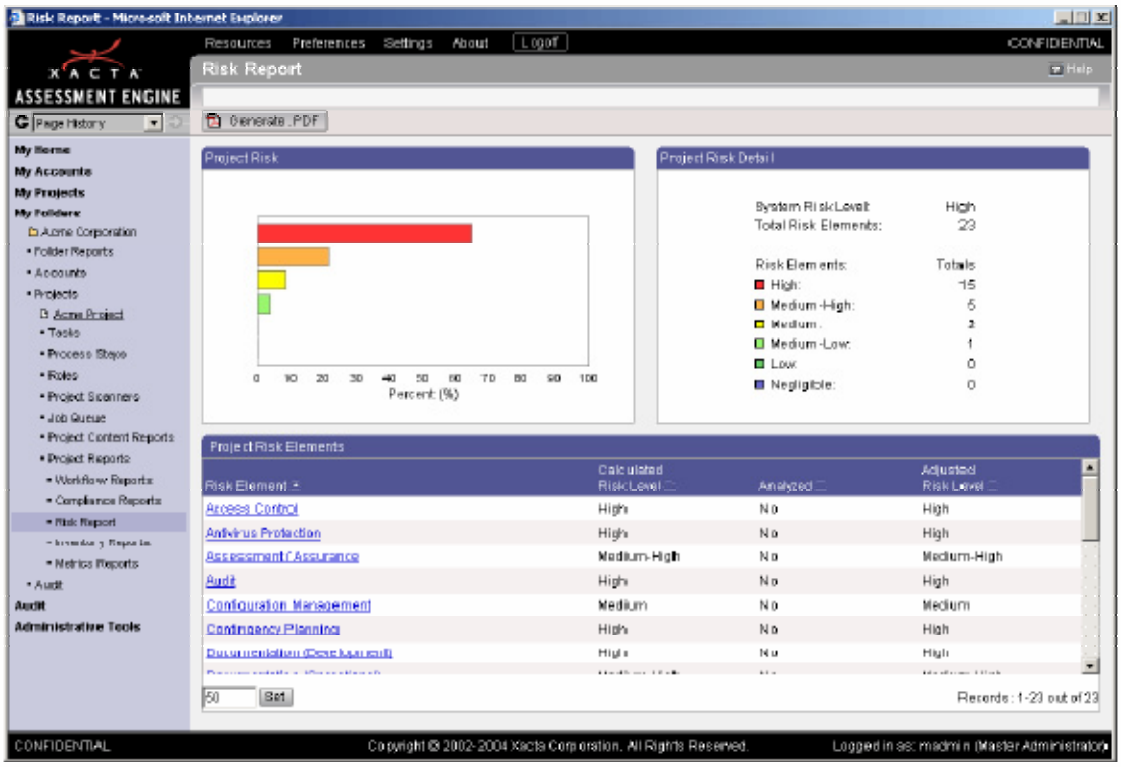


Figure 40. Risk Report
[From 18]

C. ENTERPRISE MISSION ASSURANCE SUPPORT SYSTEM (EMASS) CERTIFICATION AND ACCREDITATION SOFTWARE SOLUTION

1. System Name and Identification

System Name: Enterprise Mission Assurance Support System – Next Generation

System ID: eMASS-NG

2. System Description

The Enterprise Mission Assurance Support System – Next Generation (*e*MASS-NG) is a government-owned, Commercial-off-the-Shelf (COTS) based solution, which seamlessly integrates several capability models to support Information Assurance (IA) program management needs. *e*MASS-NG is fully compliant with the concept of IA controls-based information assurance, and is intended to provide full support of the

Department of Defense (DoD) 8500 series, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37/800-53, and Director of Central Intelligence Directives (DCID) 6/3 environments.

The Enterprise Mission Assurance Support System (*e*MASS) was originally developed as a Research and Development (R&D) prototype – this version was labeled Release 2.0. The *e*MASS development continued to Next Generation, which will be used by DoD, Civil, and Federal agencies alike.

At its core are a flexible Relational Database Management System (RDBMS) and a clear, easy-to-use web interface driven by decision wizards to perform complex functions and data analysis. Additionally, other core modules will consist of ports and protocols management, vulnerability management, configuration management, IA architecture and asset management, and other policy compliance with Defense Information Systems Agency (DISA) Standard Technical Implementation Guide (STIG) and National Security Agency (NSA) Security Recommendation Guides (SRGs).

*e*MASS-NG is designed to operate in a secure intranet, such as a logically isolated Non-classified Internet Protocol Router Network (NIPRNet) enclave or a Secret Internet Protocol Router Network (SIPRNet) enclave. The application is enabled with Public Key Infrastructure (PKI), and all data in transit, at rest, and on backup media is fully encrypted. *e*MASS-NG will provide a secure web-based system for IA professionals to automate all aspects of enterprise-wide IA planning and operations including decisions, workflow, configurations, and relationships.

a. System Diagrams

Figure 16 depicts a high level graphical representation of the overall functionality of *e*MASS-NG once it has been fully developed. Figure 17 depicts the C&A architecture of *e*MASS-NG.

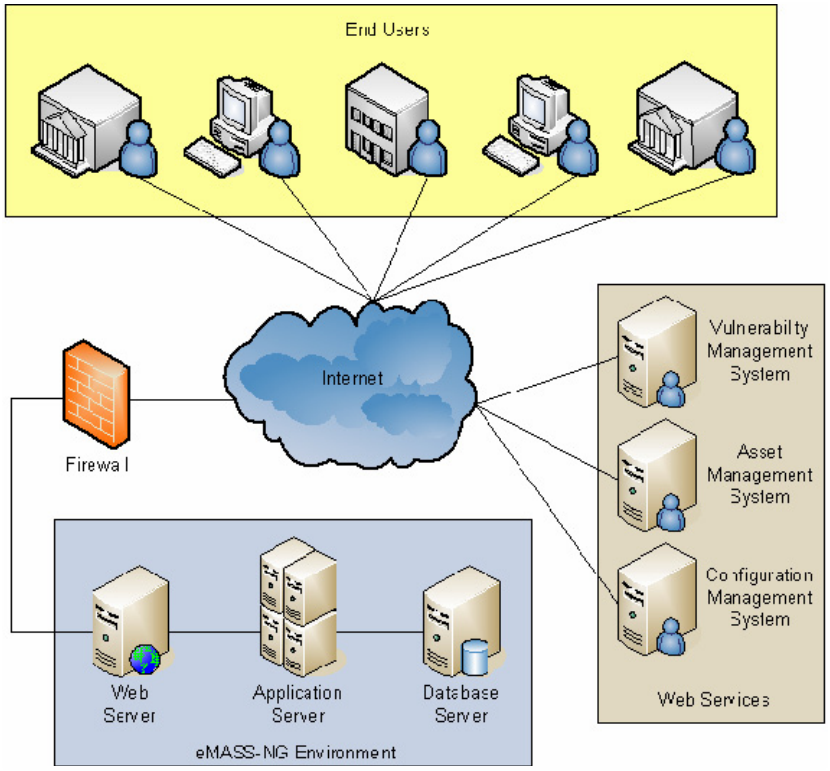


Figure 41. eMASS-NG Functionality

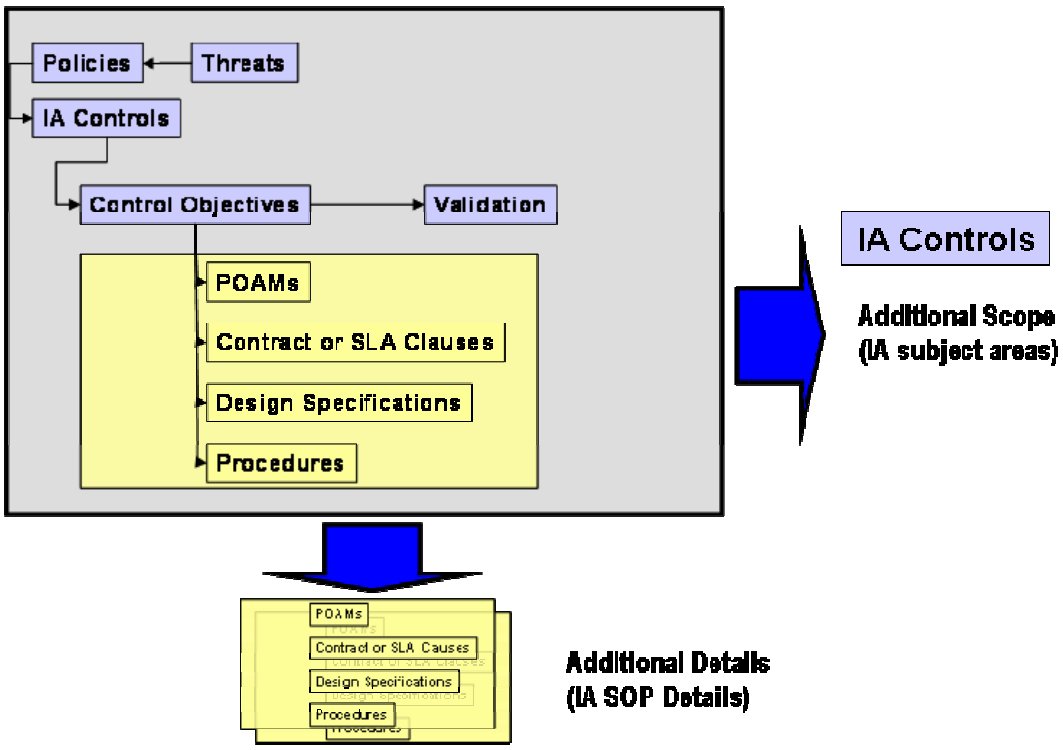


Figure 42. eMASS-NG C&A Architecture

3. Functional Description

a. System Capabilities

*e*MASS-NG will allow users to enter system information, track the progress of the information assurance activities (such as: validation tests, compliance statuses, artifacts, etc.) and associated action plans for the purpose of sharing system security information and compliance status. This system will be designed to allow members of the DoD community to track accreditation of their component systems, and provide the status of their system vulnerabilities to controlling authorities.

b. System Classification

The intent of this section is purely informational and not marketing. The purpose of the data is to inform potential C&A users that the eMASS tool is classified as a Mission Assurance Category (MAC) II, Sensitive. This information is not intended to persuade but inform potential C&A users of the facts related to the classification of the eMASS automated C&A tool.

In accordance with DoD Instruction 8500.2, this system is classified as a MAC II, Sensitive. This system is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.

c. Classification and Sensitivity of Data Processed

Information that is stored, processed, and transmitted on, through and/or from *e*MASS-NG is considered at least Sensitive But Unclassified and should be marked as For Official Use Only (FOUO). All FOUO data is protected by measures appropriate for unclassified system high operations. Need-to-know controls are an element of the protective measures placed on *e*MASS-NG. All system administration information contained in *e*MASS-NG is under the cognizance of the *e*MASS-NG Program Manager.

*e*MASS-NG is capable of profiling the certification status of Defense Information Systems Network (DISN) systems. The resulting map and profiles of DISN systems would be a valuable resource for both internal and external threat exploitation.

Exploitation of this information and/or penetration of the DISN could lead to the following:

- Unauthorized access to DoD information assets.
- Manipulation of information for unauthorized purposes, including personal gain.
- Accidental or intentional denial of services attacks to DoD information assets.
- Wrongful disclosure of sensitive certification and accreditation information.

The following matrix describes the functional data category (e.g., e-mail, network management traffic, personnel transactions, financial transactions), the data target (receiving application), the classification and sensitivity of the data (e.g., Unclassified, Privacy Act, Financially Sensitive, Proprietary, Administrative/Other, Confidential, Secret, Top Secret, Compartmented/Special Access), the user clearance level required for access, the data source (originating application), and the transmission mode (e.g., Internet, Web, File Transfer Protocol (FTP), Telnet, Stand Alone, Manual Procedure, Value Added Network(VAN)). For transmissions outside the boundary of this SSAA, the matrix also includes the protection measures in place and the accreditation status of interfacing systems or networks.

Table 5. *e*MASS-NG Data Type and Flow

Data Category	Receiving System	Data Type	Clearance Level	Data Source	Transmission Mode	Protection Mechanism	C&A Status
Connectivity	WAN	Administrative	Non-sensitive	N/A	Intranet, LAN, WAN	Network Perimeter Components	Unknown
Firewall Logs	Cisco PIX Firewall	Administrative	Non-sensitive	Firewall, Internet	Internet, Web, FTP, Telnet, Stand Alone, LAN, VAN, WAN	Network Perimeter Components	N/A
Intrusion Detection Log File	Router, Cisco PIX Firewall, IDS	Administrative	Non-sensitive	Internal/ External Networks	Intranet, Internet, Web, FTP, Telnet, LAN, VAN, WAN	Network Perimeter Components	N/A
Network Management Traffic	Router, Cisco PIX Firewall, IDS	Administrative	Non-sensitive	Internet, Web, FTP, Telnet, LAN, VAN, WAN	Internet, Web, FTP, Telnet, LAN, VAN, WAN	Network Perimeter Components	N/A

d. System User Description and Clearance Levels

The users of these systems can be divided into four groups:

1. Guest User - An individual who is granted access to the system login page and has the ability to register for access.
2. Registered User - An individual who is granted access to the system.
3. Administrator - An individual responsible for the configuration of the eMASS-NG system for a specific server box. This individual will be assigned the responsibilities of defining the organizational hierarchies, role/permission groupings, workflows, and system settings.
4. Primary Author - An individual who is responsible for managing the documentation of a system. This individual will be assigned the responsibilities of editing controls, editing validation tests and editing expected results.

A user profile and a role must be created for every user within the eMASS-NG instance in order for them to access eMASS-NG. The system registration process begins when a user accesses the eMASS-NG public site and creates a user profile. Once the user has entered the required information, this data is passed to the system and appears on the workload of the system administrator. The system administrator must then manually verify that the user requesting access to eMASS-NG has been assigned a role by the organization's approval authority. If so, the system administrator activates the user and sends a response to the user, indicating that their account is now active. If the user has not been assigned a role, the user must wait for their role to be assigned. If the organization's approval authority denies a role assignment to a user requesting access, the system administrator will deny the registration request and notify the user that their request was denied.

The clearance level of this system is unclassified. All users of this system will have the proper level of security clearance to operate, at a minimum, in a user capacity on the system. Additionally, all users have the appropriate clearance level to perform their specific duties. Federal employees have undergone the appropriate hiring screening process associated with their position. Contractors are required to complete a Standard Form 86 from which a National Agency Check with Inquiries (NACI) is conducted.

e. Life Cycle of the System

*e*MASS-NG is in the development stage of its life cycle. It is an R&D project funded by the Office of the Assistant Secretary of Defense Networks and Information Integration (ASDNII). Its purpose is to provide full automation support for the next generation of information assurance policy, the DoD 8500 series. It utilizes DoD's proven e-business automation techniques to take information assurance management to the next level. *e*MASS-NG is an enterprise-wide solution for IA management.

The configuration and operation of *e*MASS-NG conforms to the life cycle design and execution strategy required for all DoD owned systems. The acquisition, installation, and testing of appropriate security software were accomplished followed by system, security, and user application testing and acceptance. *e*MASS-NG will be subjected to a periodic Security Readiness Review (SRR) process to ensure the integrity, confidentiality, availability, and accountability of the system and its data.

f. Minimum System Requirements

eMASS-NG is configured using Microsoft Windows 2000 and UNIX based servers to support web access from DoD approved web browsers hosted on appropriately managed client workstations.

Network Deployment

The following are the minimum hardware requirements for an eMASS multi-server installation:

Load Balancer

Catalyst Switch

8 Port Fiber Channel Switch

Power Vault Storage Area Network (SAN)

Cisco Pix Firewall

(Two) Web Servers functioning as UNIX servers.

- Dell PowerEdge 2650 with 2 Intel Xeon Processors (2.0-3.2 GHz) with hyper threading support
- 1-12 GB PC266 ECC DDR SDRAM RAM

- Raid Controller Embedded dual channel Ultra 3 (U160) SCSI with 128 MB cache
- 730 GB (5 x 146GB) Hard Drive
- MS Office 2000, MS Office XP, MS Office 2003
- MSDE or MS SQL Server 2000 (Service Pack 3 or above) or Oracle 8i/9i/10g
- MS Windows 2003 Server
- Windows External Connector
- Crystal Reports 10

Database Servers

- Dell PowerEdge 2650 with 2 Intel Xeon Processors (2.0-3.2 GHz) with hyper threading support
- 1-12 GB PC266 ECC DDR SDRAM RAM
- Raid Controller Embedded dual channel Ultra 3 (U160) SCSI with 128 MB cache
- 730 GB (5 x 146GB) Hard Drive
- MS Office 2000, MS Office XP, MS Office 2003
- MSDE or MS SQL Server 2000 (Service Pack 3 or above) or Oracle 8i/9i/10g
- MS Windows 2003 Server

Desktop/Laptop

- Pentium 4 (2 GHz Processor)
- 1 GB RAM
- 40 GB Hard Drive
- MS Office 2000, MS Office XP, MS Office 2003
- MSDE or MS SQL Server 2000 (Service Pack 3 or above) or Oracle Client 9.2
- MS Windows 2000 Server/Pro or MS Windows XP Pro or MS Windows 2003 Server

The following are the minimum software requirements for an eMASS multi-server installation:

eMASS Web Servers functioning as UNIX servers.

- MS Windows 2000 Advanced Server, SP4, SSL connection, using Kernel Modes
- MS DotNet Framework, SP1, Standard, Not Kernel Mode
- MS IIS Diagnostics, 1.0, Standard, Not Kernel Mode
- Crystal Reports,10, Standard, Not Kernel Mode
- Symantec Antivirs, 8.1, Standard, Not Kernel Mode

eMASS SQL Stage Server

- MS Windows 2000 Advanced Server, SP4, SSL connection, using Kernel Mode
- MS DotNet Framework, SP1, Standard, Non Kernel Mode
- MS IIS Diagnostics, 1.0, Standard, Non Kernel Mode
- MS SQL Server, SP 3a, Standard, Kernel Mode
- Symantec Antivirs, 8.1, Standard, Non Kernel Mode

eMASS SQL Web –Enabled Database Server

- Oracle Client, 9.2, Non Kernel Mode
- Oracle Universal Installer, 2.2.0.12.0, Standard, Non Kernel Mode
- MS Windows 2000 Advanced Server, SP4, SSL connection, using Kernel Modes
- MS DotNet Framework, SP1, Standard, Non Kernel Mode
- MS IIS Diagnostics, 1.0, Standard, Non Kernel Mode
- MS SQL Server, SP 3a, Standard, Kernel Mode
- Symantec Antivirs, 8.1, Standard, Non Kernel Mode

eMASS Oracle Server

- Oracle Client, 9.2, Kernel Mode
- Oracle Universal Installer, 2.2.0.12.0, Non Kernel Mode
- MS Windows 2000 Advanced Server, SP4, SSL connection, using Kernel Modes
- MS DotNet Framework, SP1, Standard, Non Kernel Mode
- MS IIS Diagnostics, 1.0, Standard, Non Kernel Mode
- MS SQL Server, SP 3a, Standard, Kernel Mode
- Symantec Antivirs, 8.1, Standard, Non Kernel Mode
- Sun J2EE SDK, 1.4, Standard, Non Kernel Mode
- WinZip 8.1, Standard, Non Kernal Mode

4. eMASS Graphic User interface (GUI)

a. Getting started with eMASS

The creation of user accounts allow users to access the eMASS system. It is the responsibility of the system administrator to approve and register new accounts in the eMASS system. The system administrator also maintains existing accounts that allow users to access the system and modify user profiles as necessary.

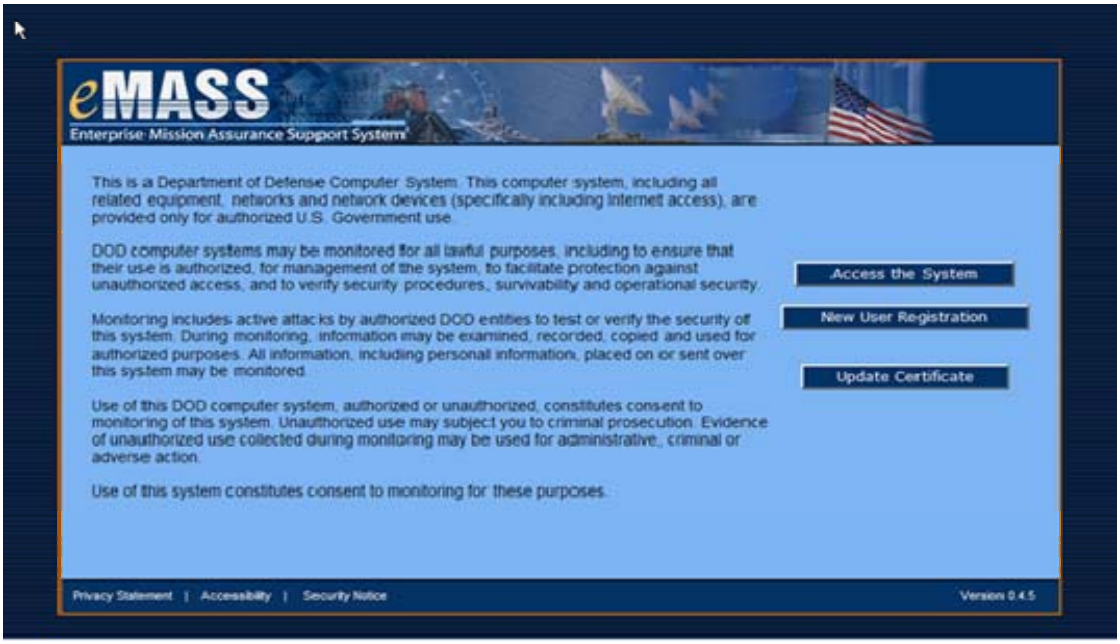


Figure 43. eMASS New User Registration
[From 16]

After the eMASS welcome banner screen, a standard security alert and a client authentication screen appears. eMASS uses Public Key Infrastructure (PKI) for authenticating its users.

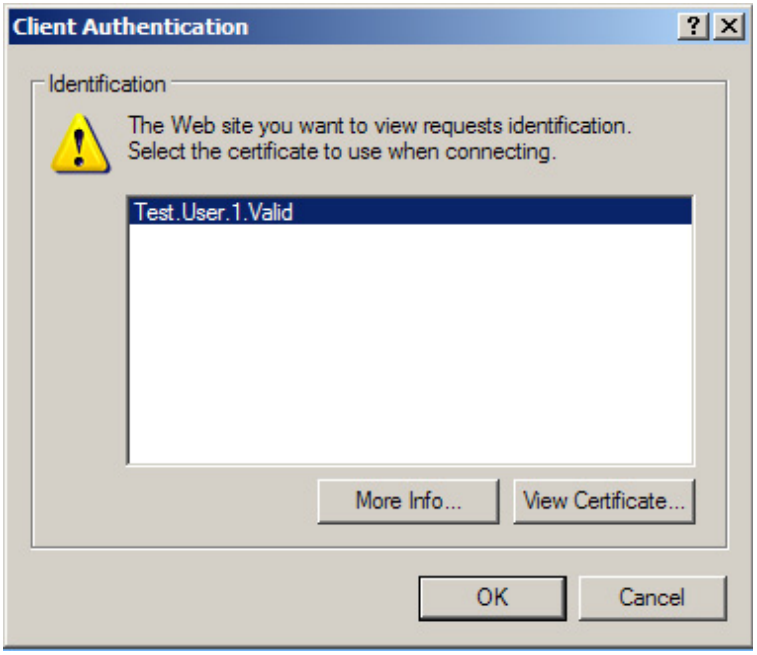


Figure 44. eMASS User Account Client Authentication (PKI)
[From 16]

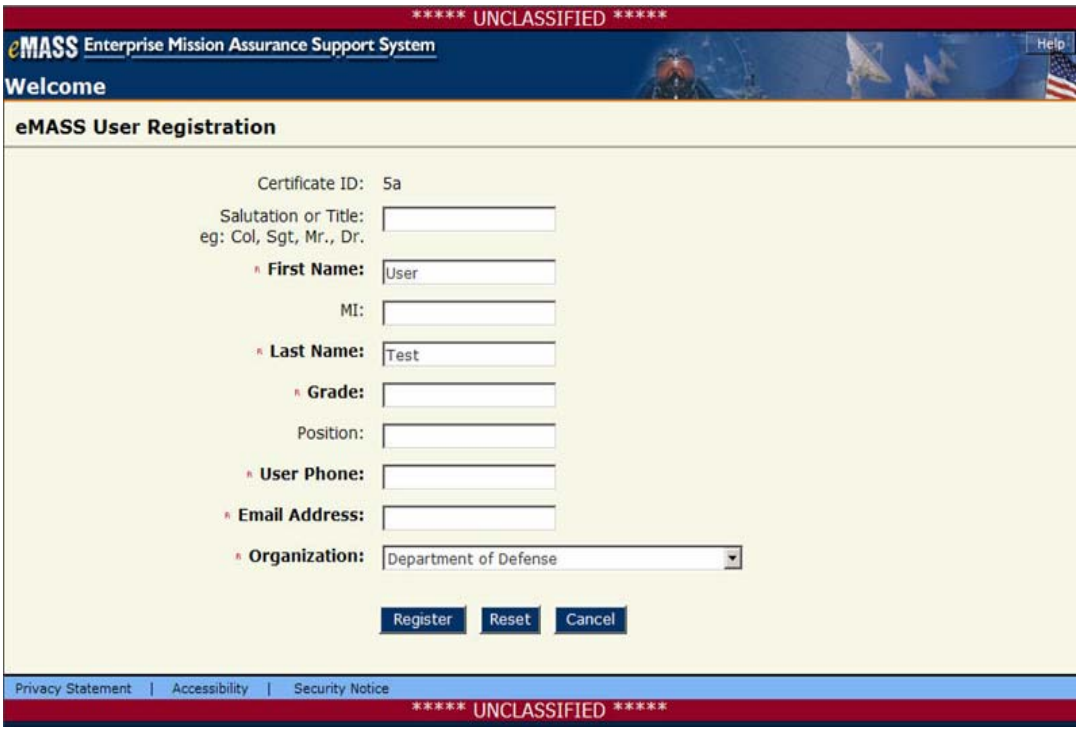


Figure 45. eMASS User Registration Application Form
[From 16]

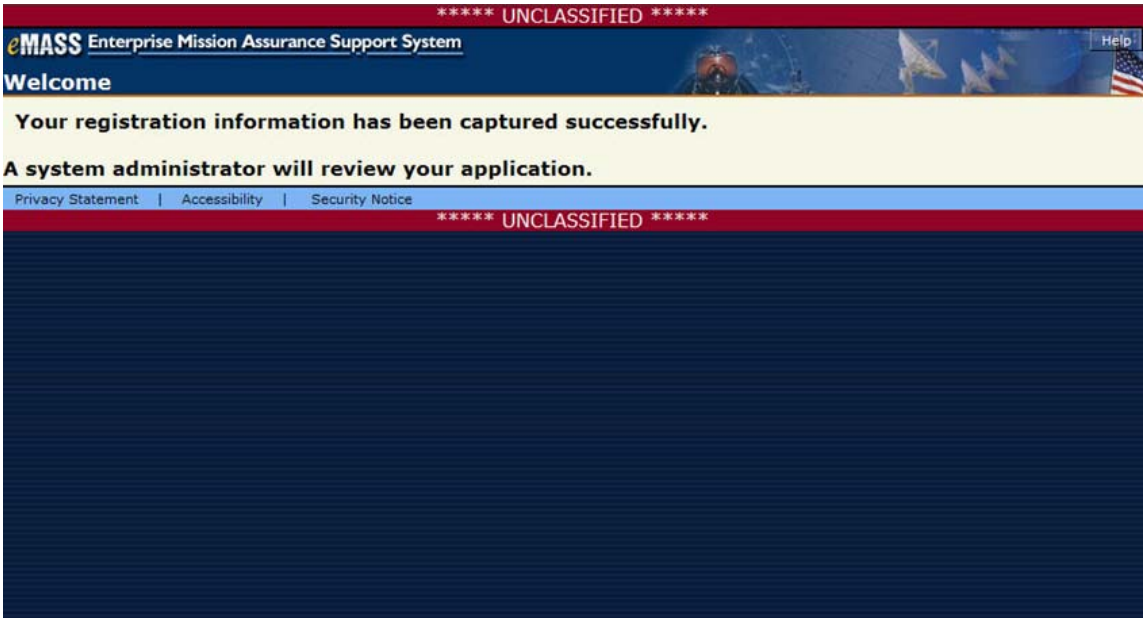


Figure 46. eMASS User Registration Confirmation
[From 16]

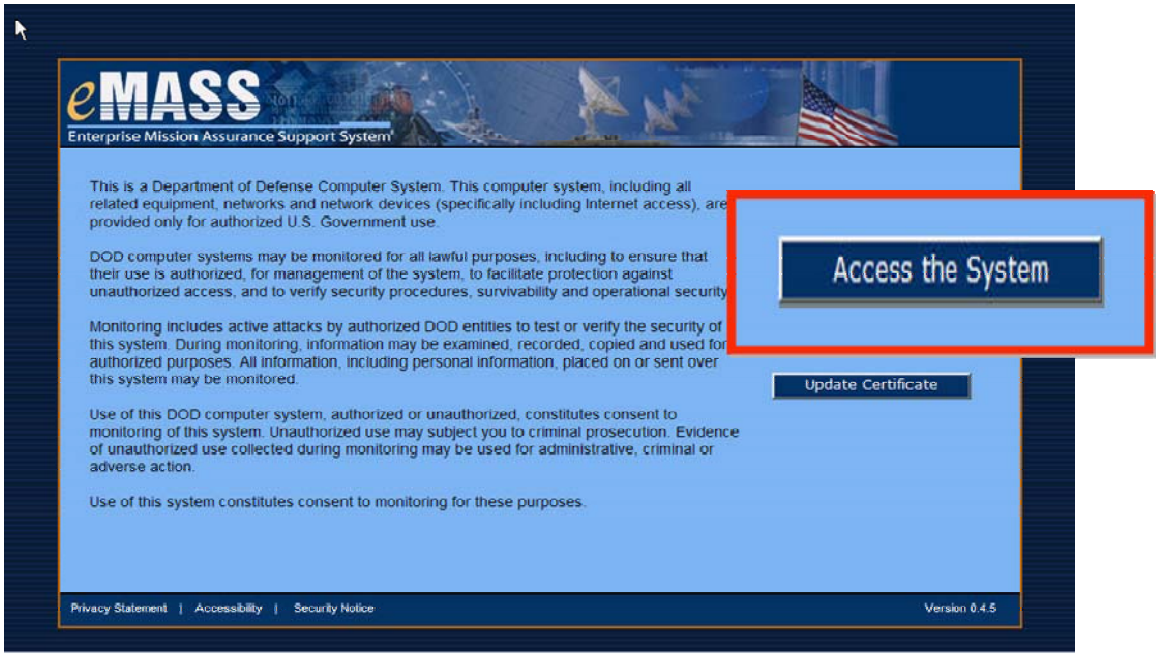


Figure 47. eMASS Existing User Account Banner
[From 16]

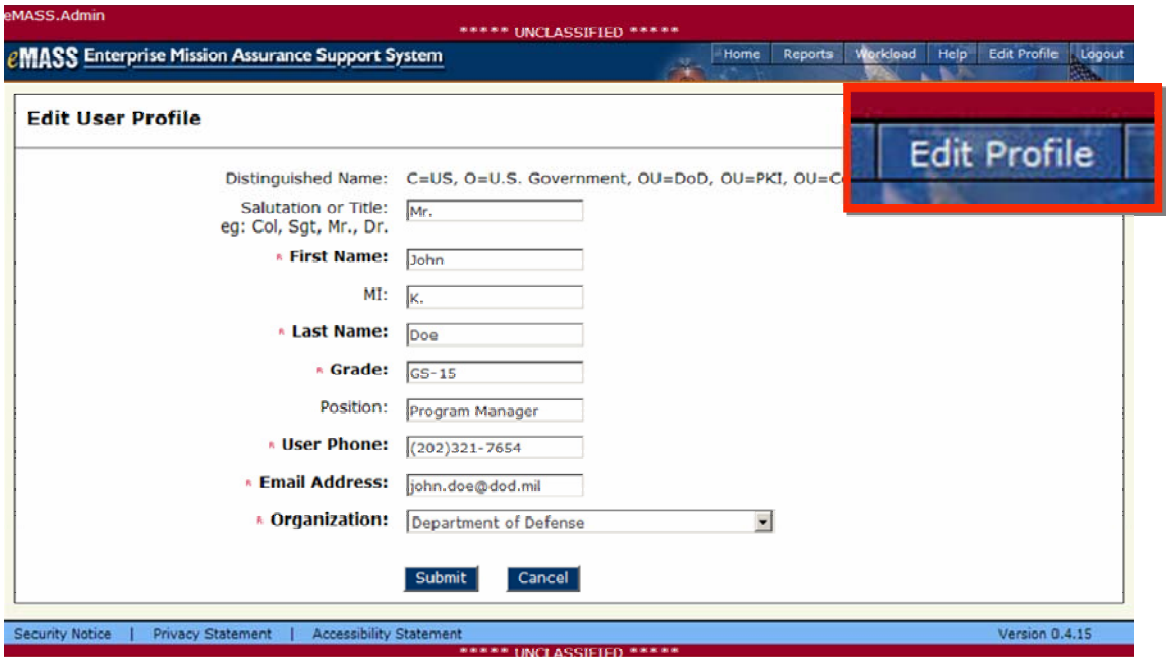


Figure 48. eMASS Existing User Edit Profile
[From 16]

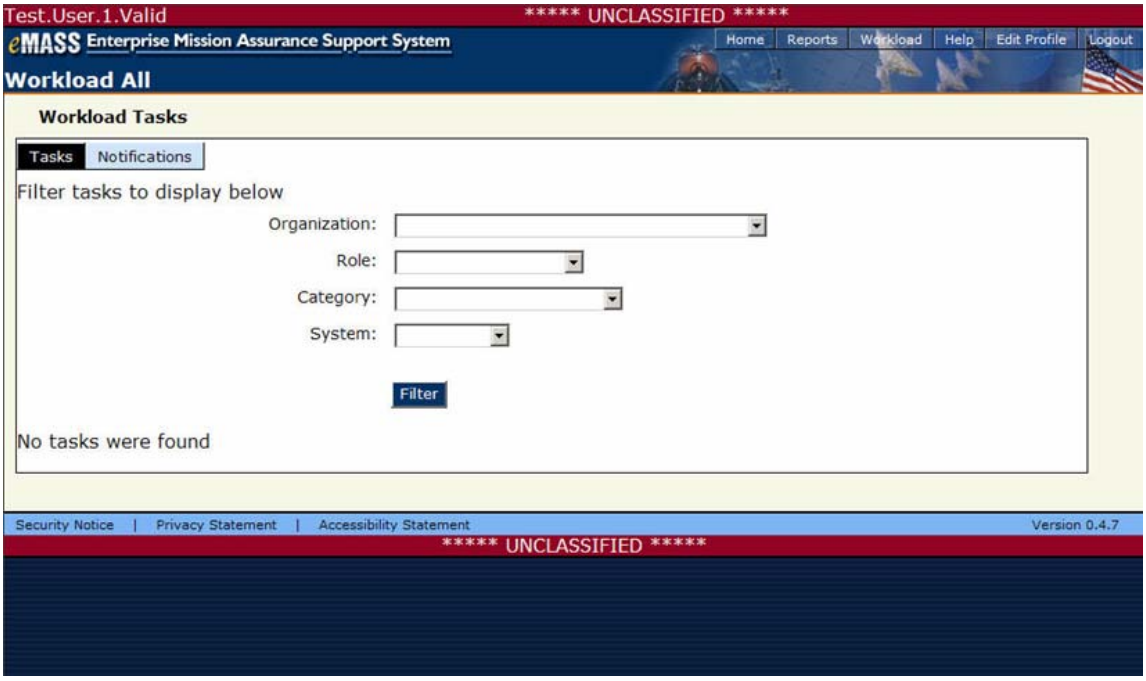


Figure 49. eMASS Navigating Workload Tasks
[From 16]

b. eMASS Controls Administration (CAM)

The eMass Controls Administration Module (CAM) permit users to (1) author and manage information assurance (IA) control sets, subject areas, and controls applicable to the following levels: the DoD Enterprise, the DoD Component, or the DoD Information System, (2) attach implementation guidance to IA controls as reference material while implementing C&A, (3) author generic validation procedures and expected results for IA controls and (4) generate controls reports to identify residual risk or areas requiring remedial action.

Instruments that measure IA condition of integrity, availability or confidentiality are called IA Controls.. These controls are achieved through the application of safeguards or regulation of specific activities. The control conditions are testable and compliance is measurable. The necessary activities required to achieve implementation of the IA control are assignable and accountable tasks.

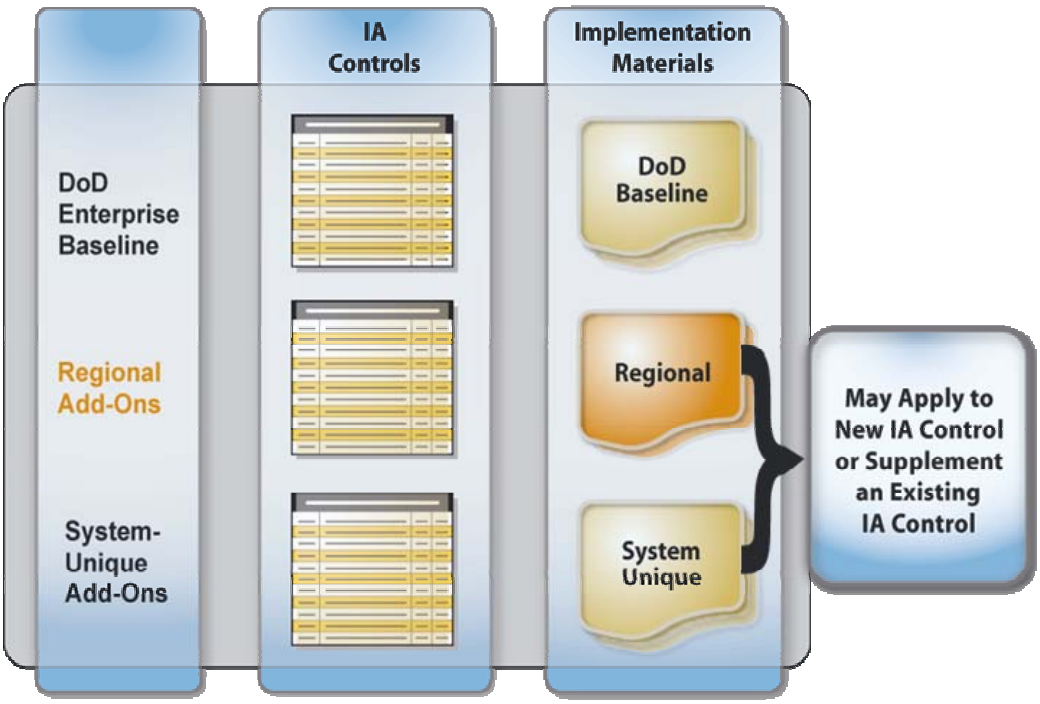


Figure 50. eMASS Role of Information Assurance (IA) controls [From 16]

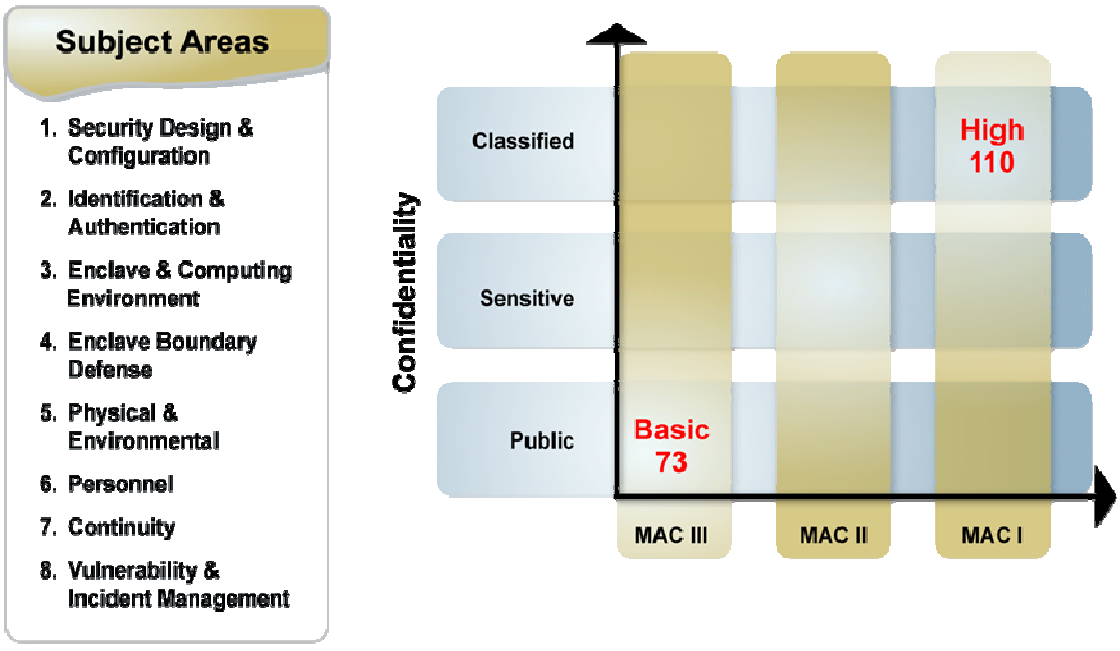


Figure 51. eMASS IA Controls MAC and Confidentiality [From 16]

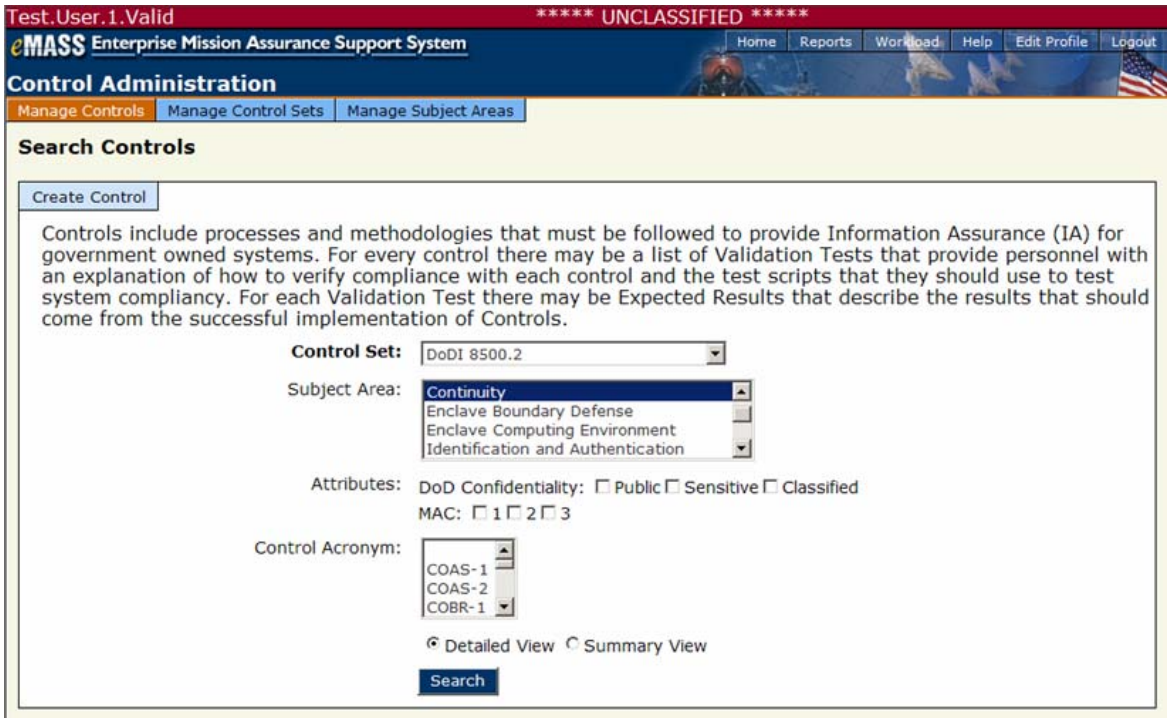
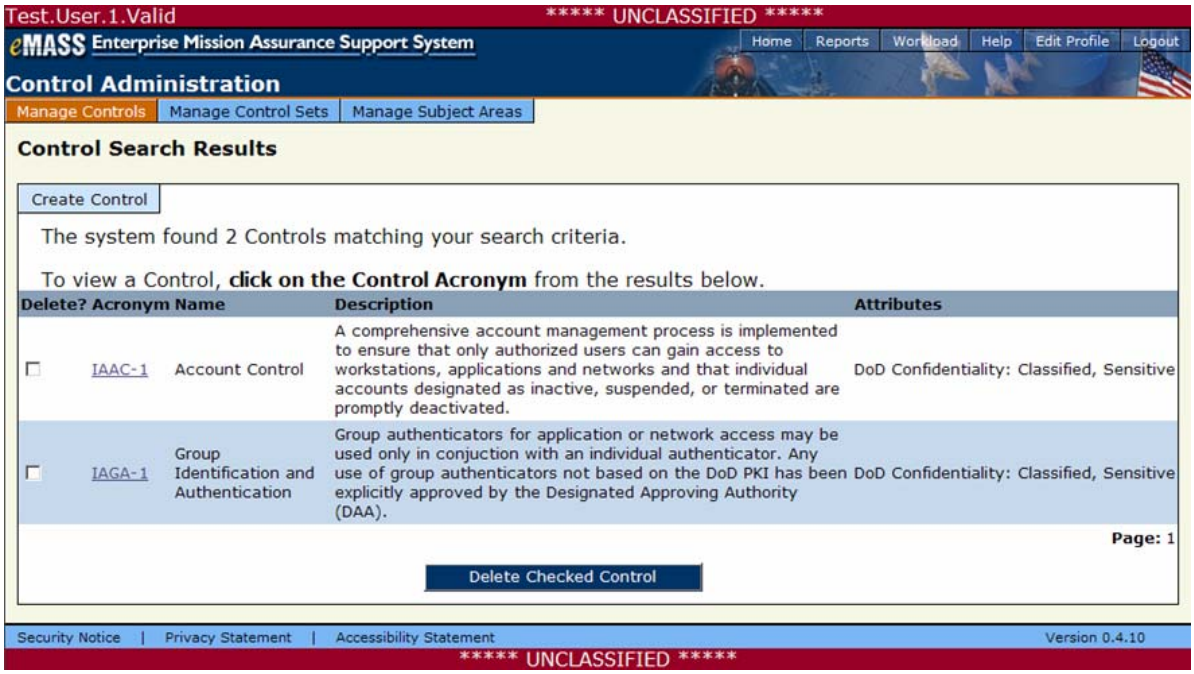


Figure 52. eMASS Managing and Searching for Controls
[From 16]



eMASS Managing and Searching for Controls (continued)
[From 16]

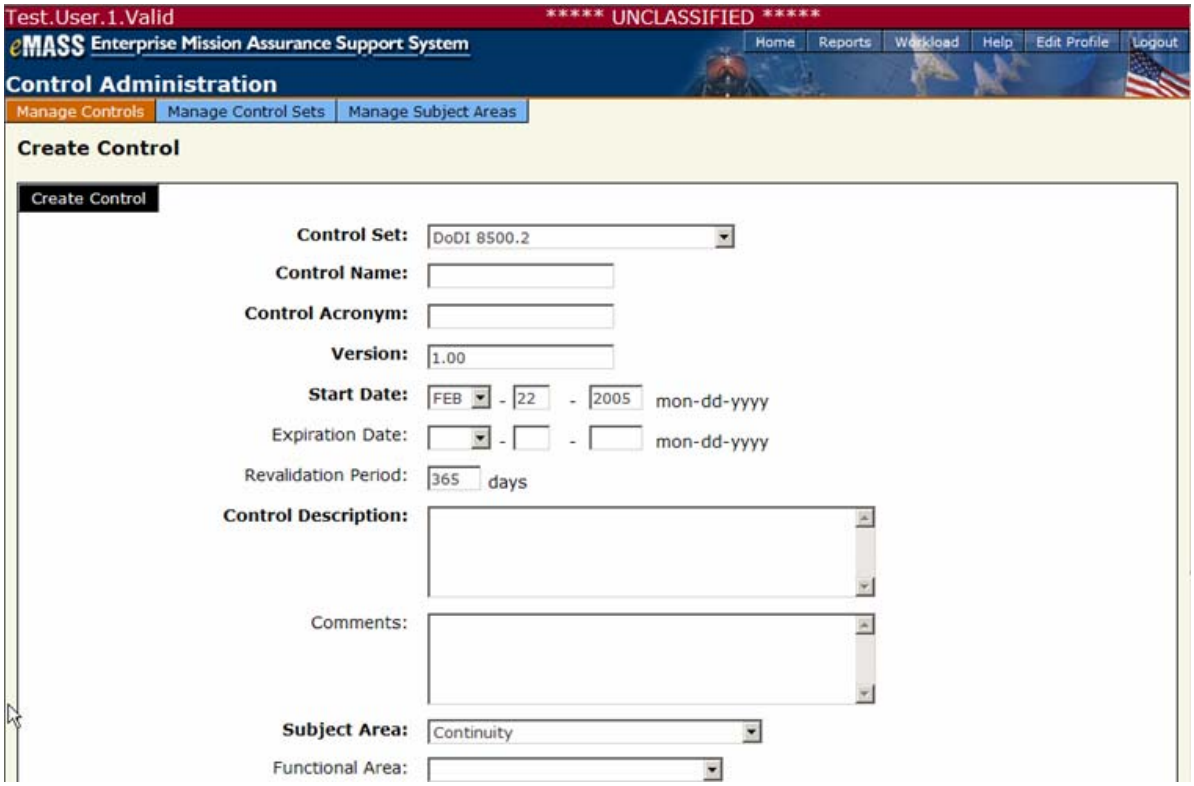


Figure 53. eMASS Managing and Creating a Control
[From 16]

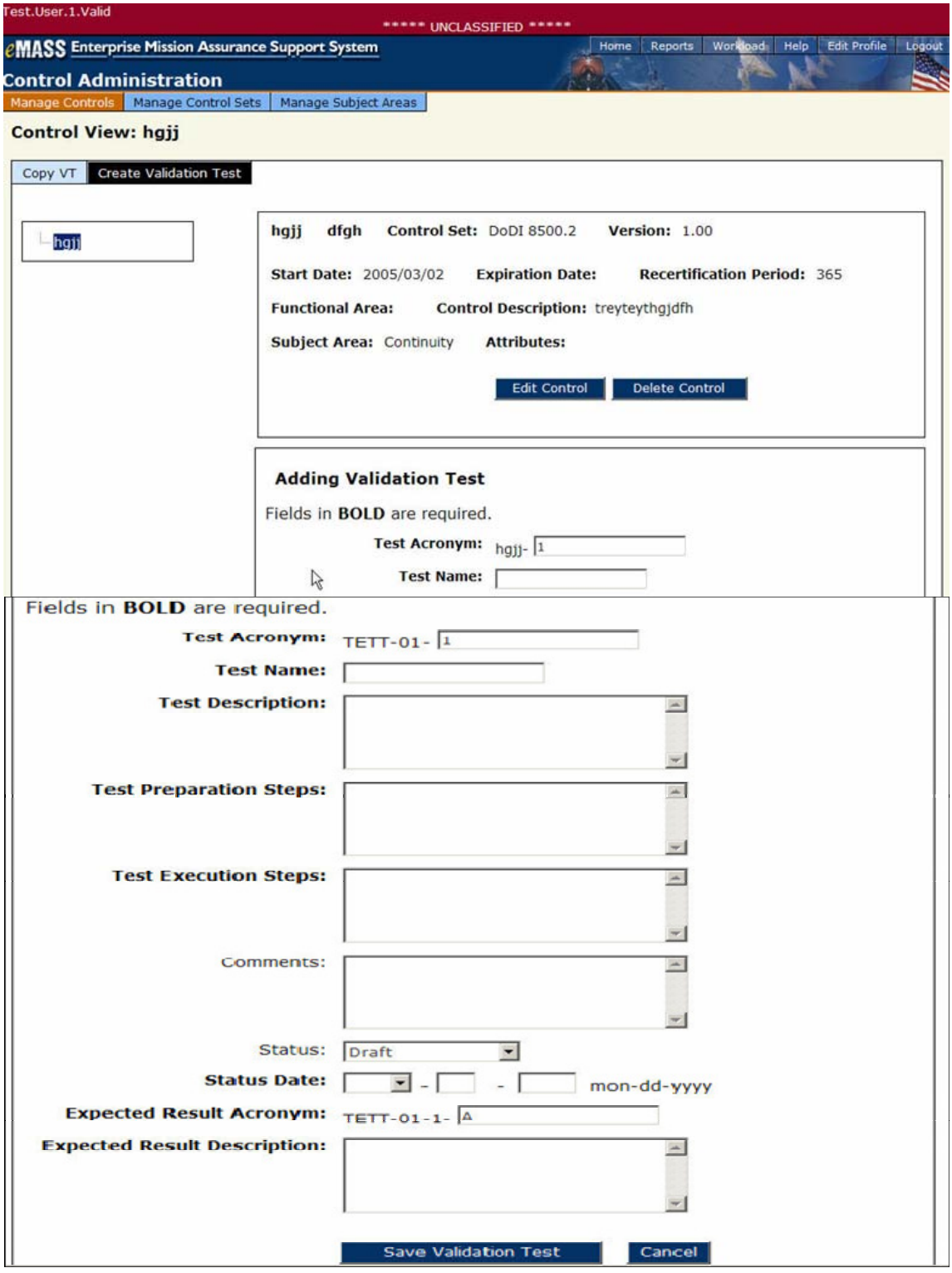


Figure 54. eMASS Creating a Validation Test
[From 16]

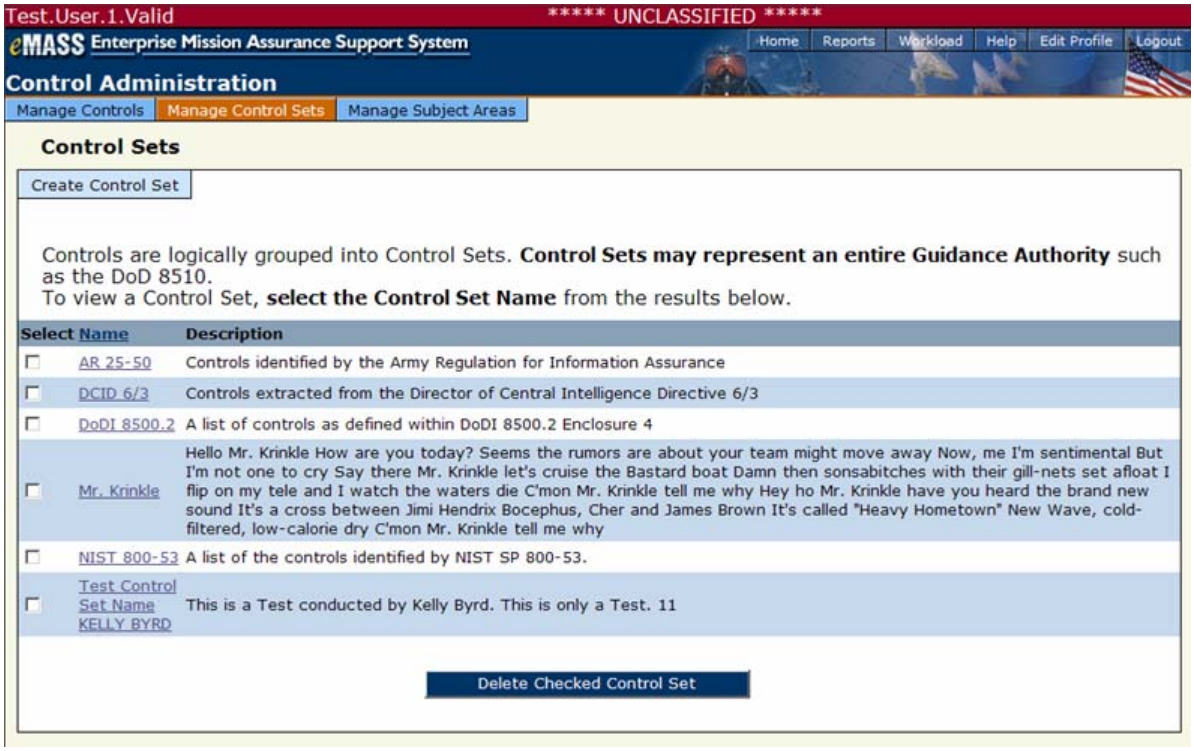


Figure 55. eMASS Managing Control Sets
[From 16]

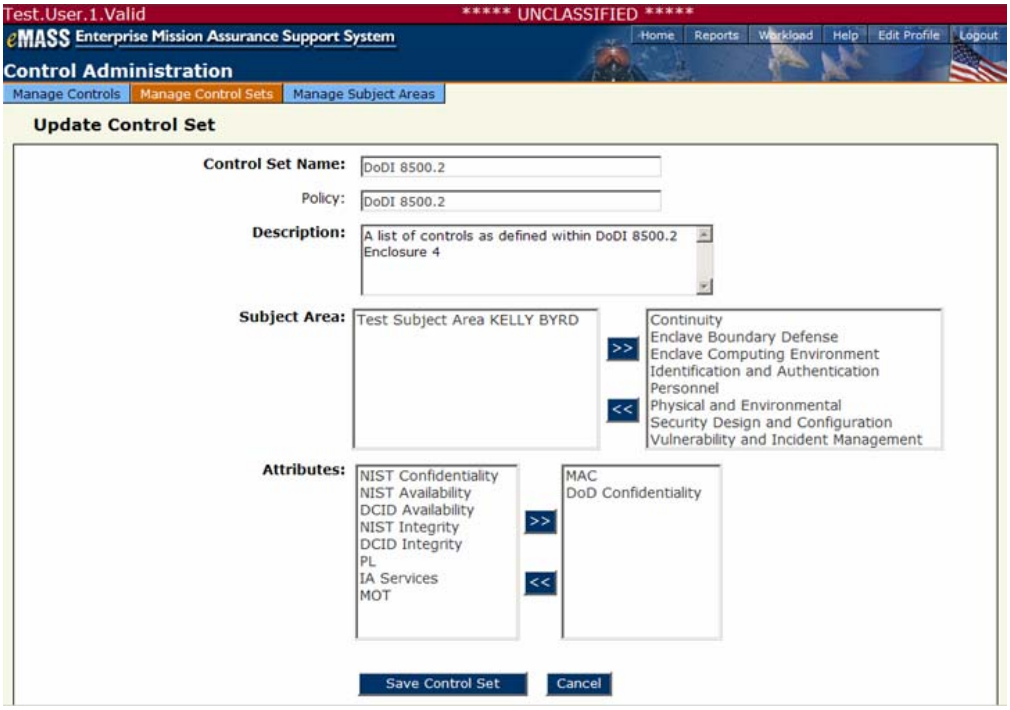


Figure 56. eMASS Updating Control Sets
[From 16]

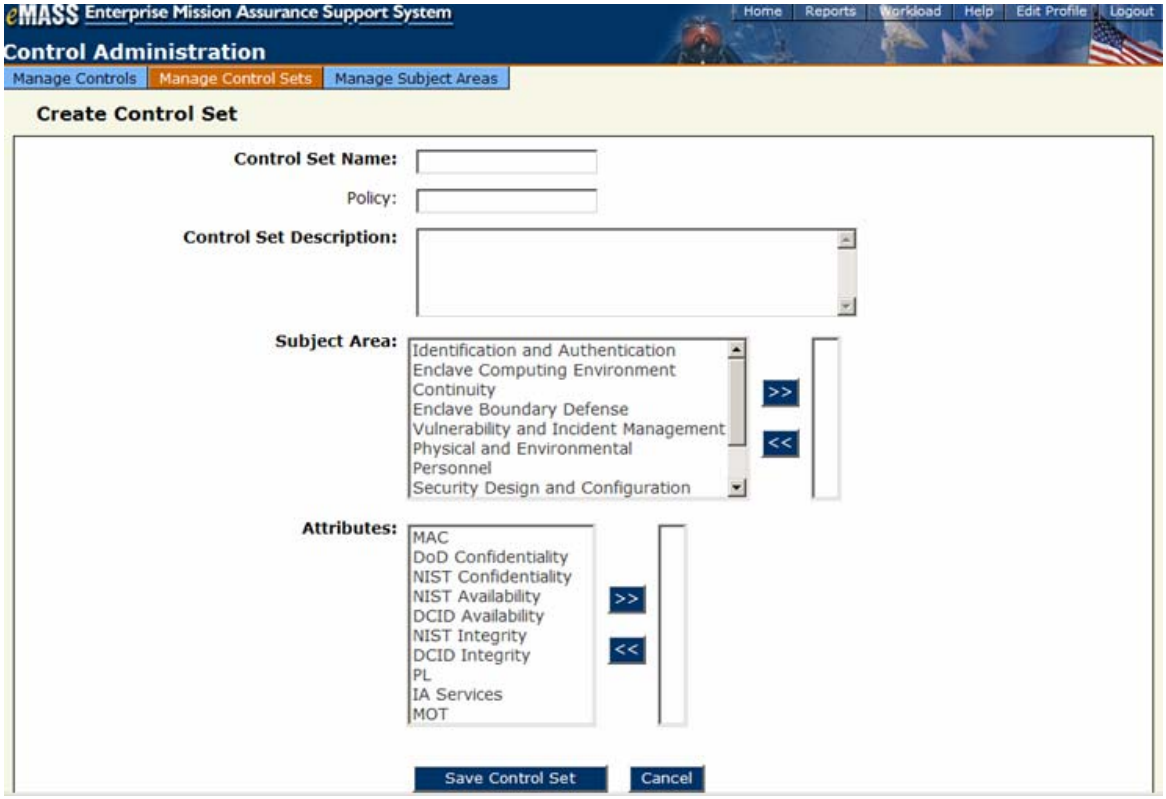


Figure 57. eMASS Creating Control Sets
[From 16]

c. eMASS Certification and Administration Module

The eMASS C&A Module provides users access to (1) view systems within eMASS with which the user has appropriate access, (2) Register new systems following the IT registration process, (3) Monitor and manage controls and their corresponding validation procedures and (4) Interact with systems as they go through workflow process.

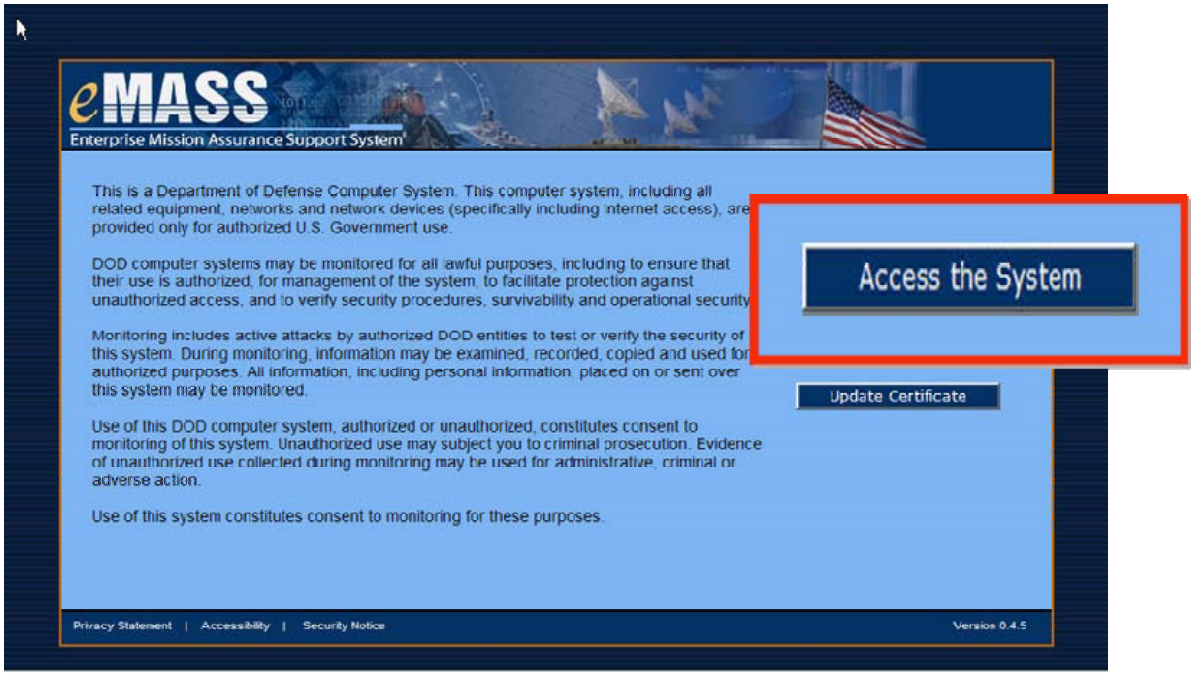


Figure 58. eMASS Certification and Accreditation (C&A) Accessing Existing User Accounts
[From 16]

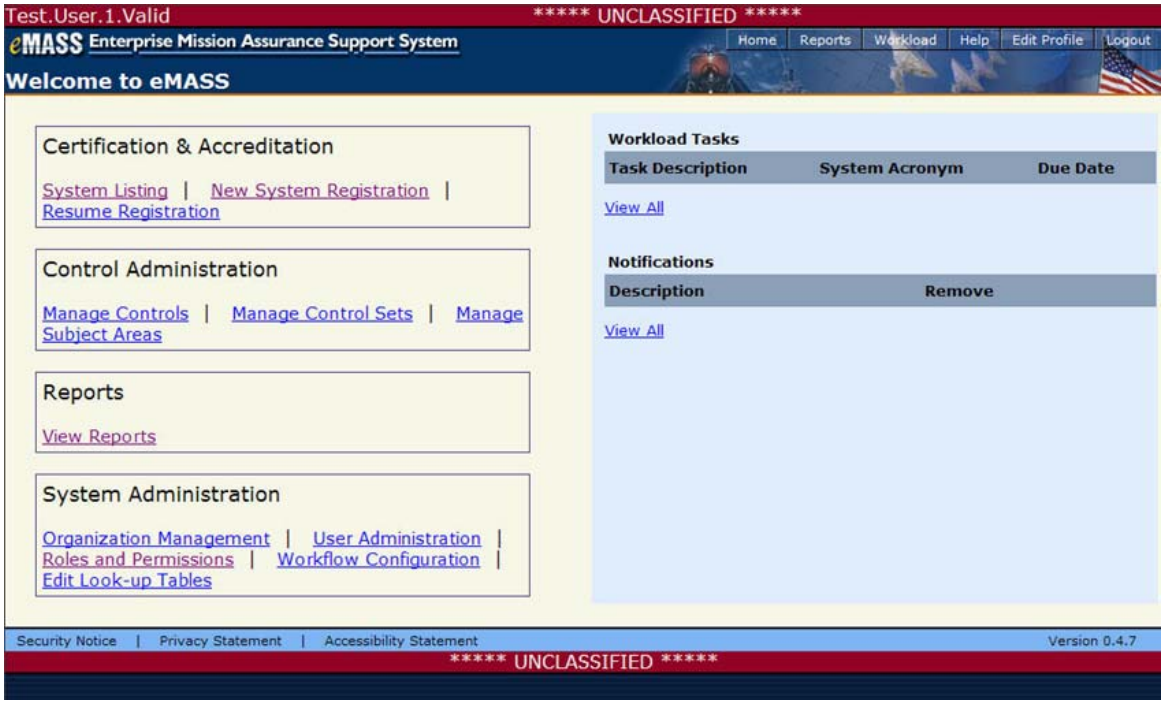


Figure 59. eMASS Certification and Accreditation (C&A) Home Page
[From 16]

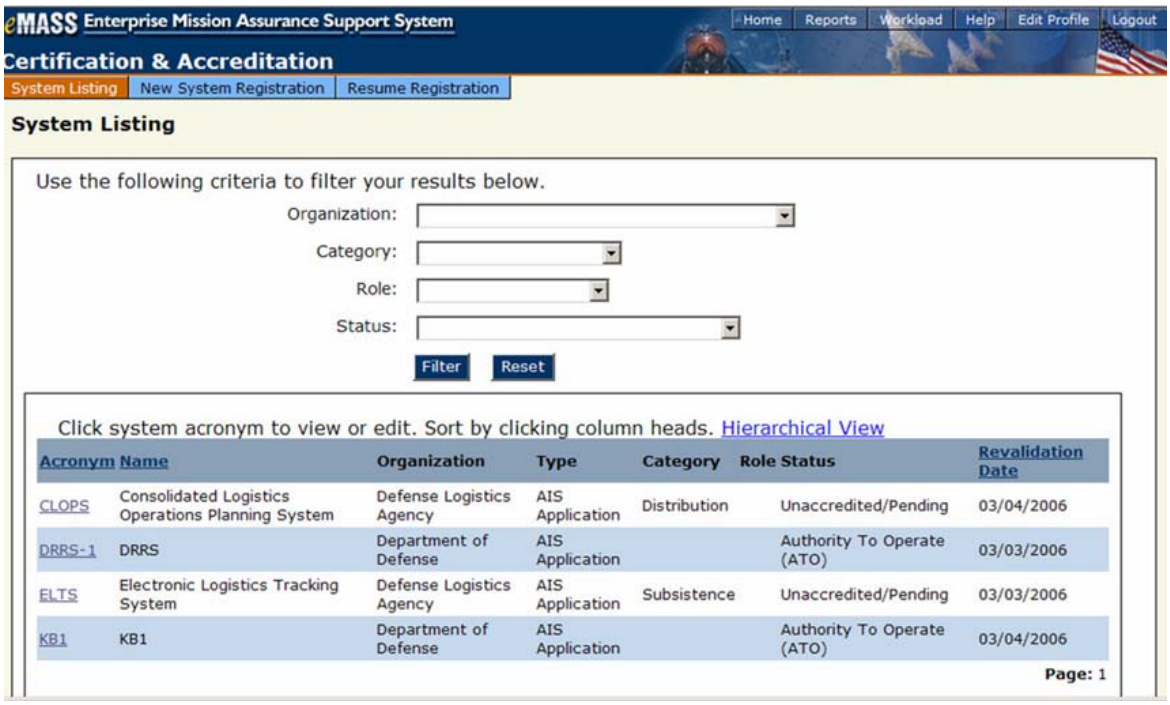


Figure 60. eMASS Certification and Accreditation (C&A) System Listing [From 16]

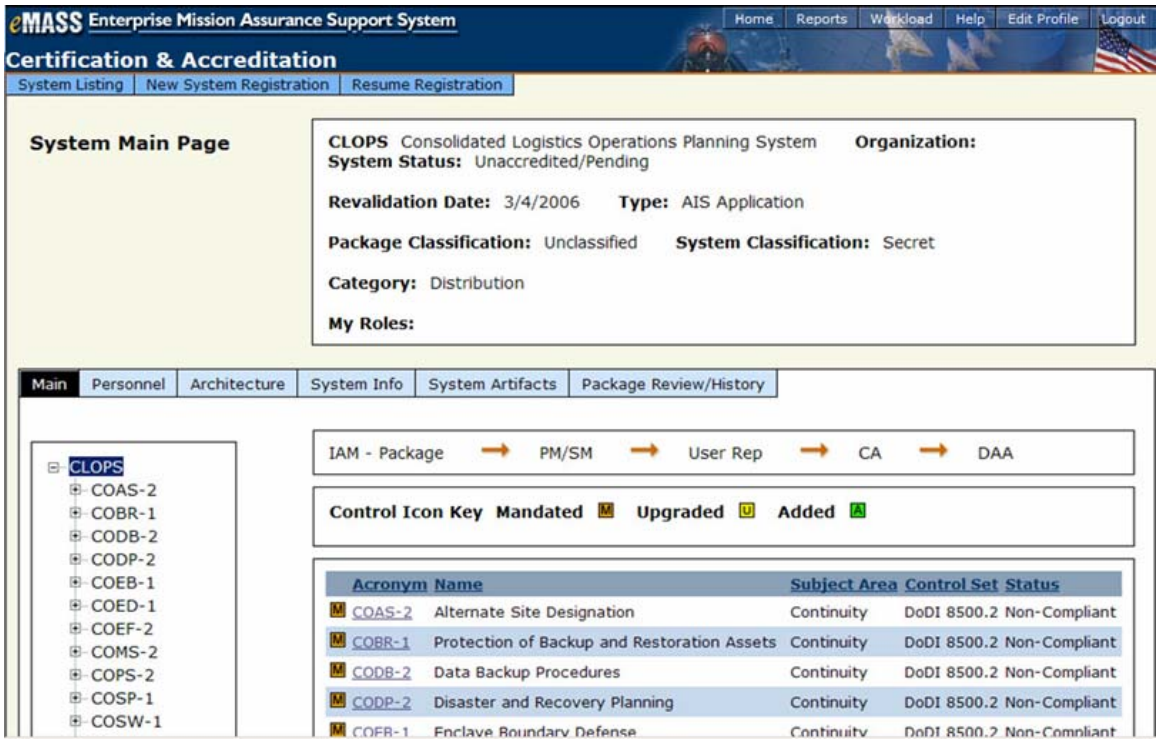


Figure 61. eMASS Certification and Accreditation (C&A) System Main Page [From 16]

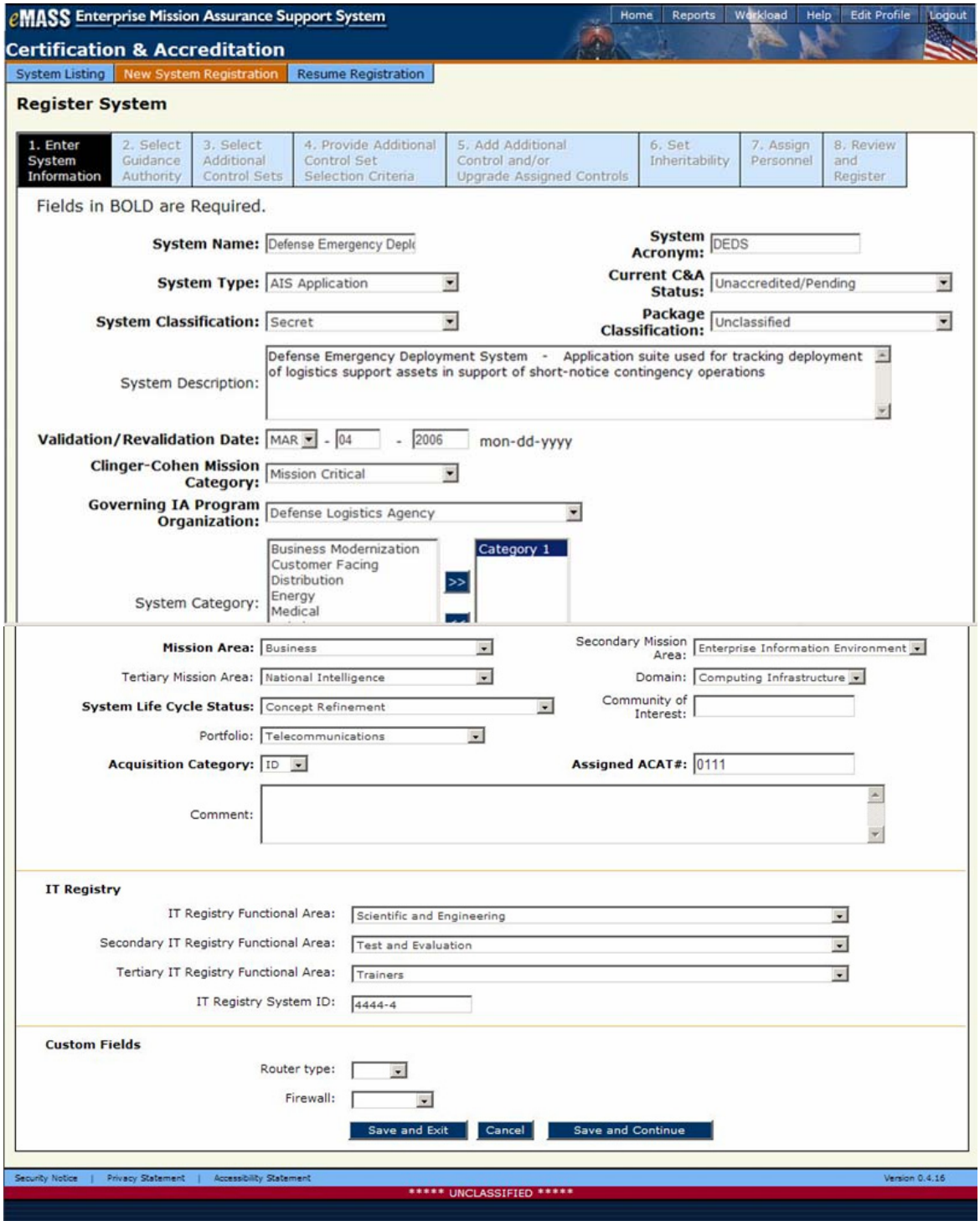


Figure 62. eMASS Certification and Accreditation (C&A) Register System [From 16]

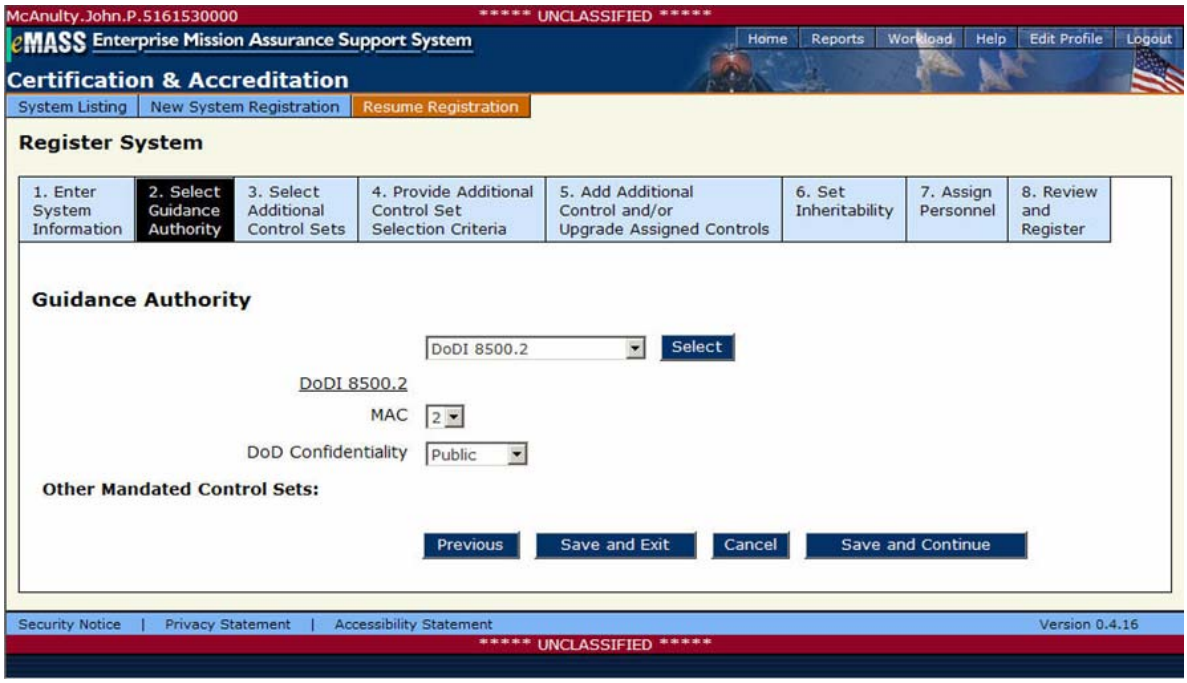


Figure 63. eMASS Certification and Accreditation (C&A) Selecting Guidance Authority [From 16]

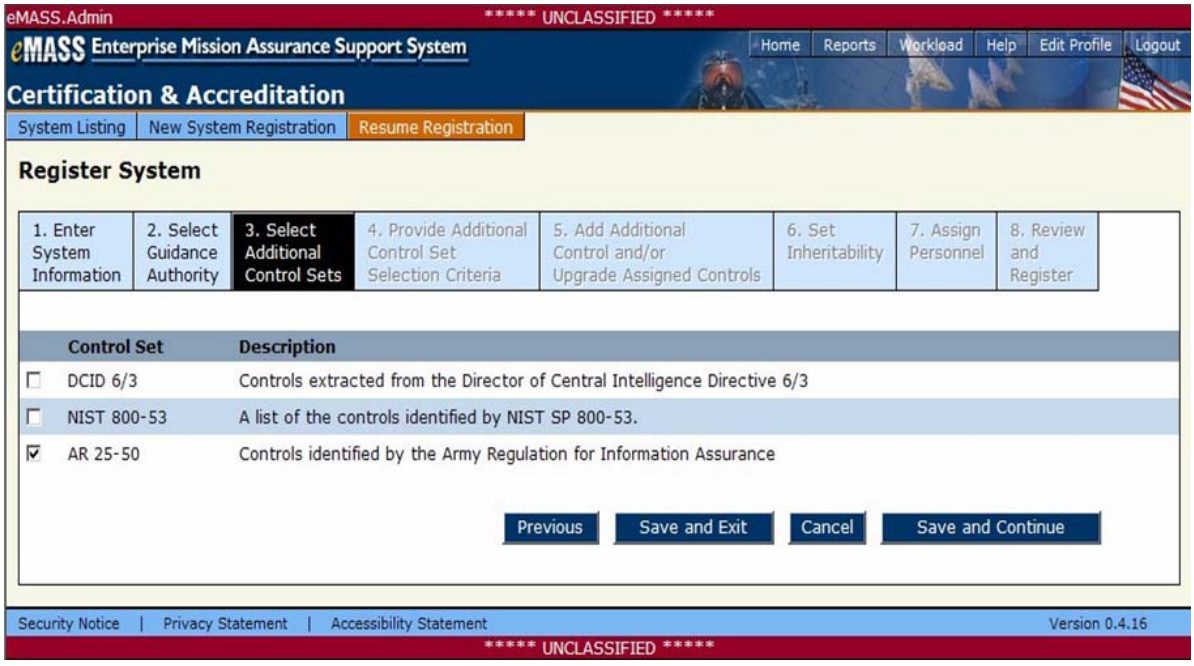


Figure 64. eMASS Certification and Accreditation (C&A) Selecting Additional Control Sets [From 16]

Figure 65. eMASS Certification and Accreditation (C&A) Selecting Additional Control Set Selection Criteria
[From 16]

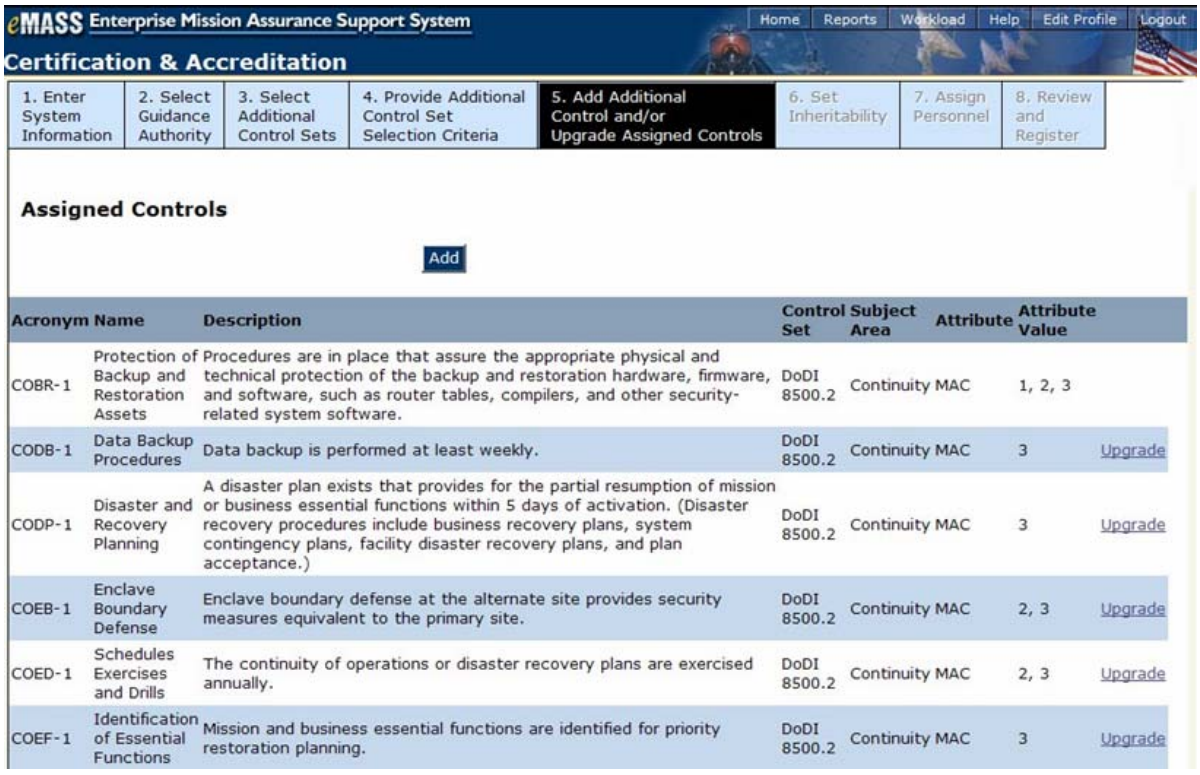


Figure 66. eMASS Certification and Accreditation (C&A) Adding and/or Upgrading Assigned Controls
[From 16]

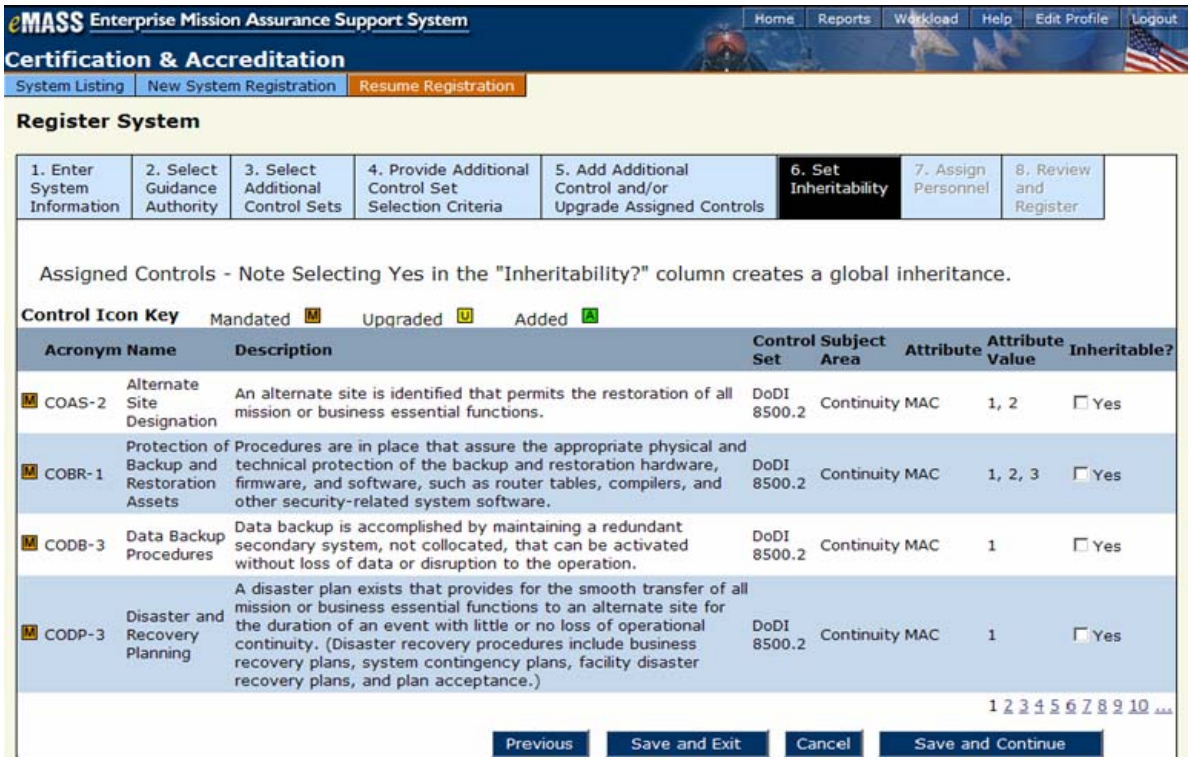


Figure 67. eMASS Certification and Accreditation (C&A) Set Inheritability [From 16]

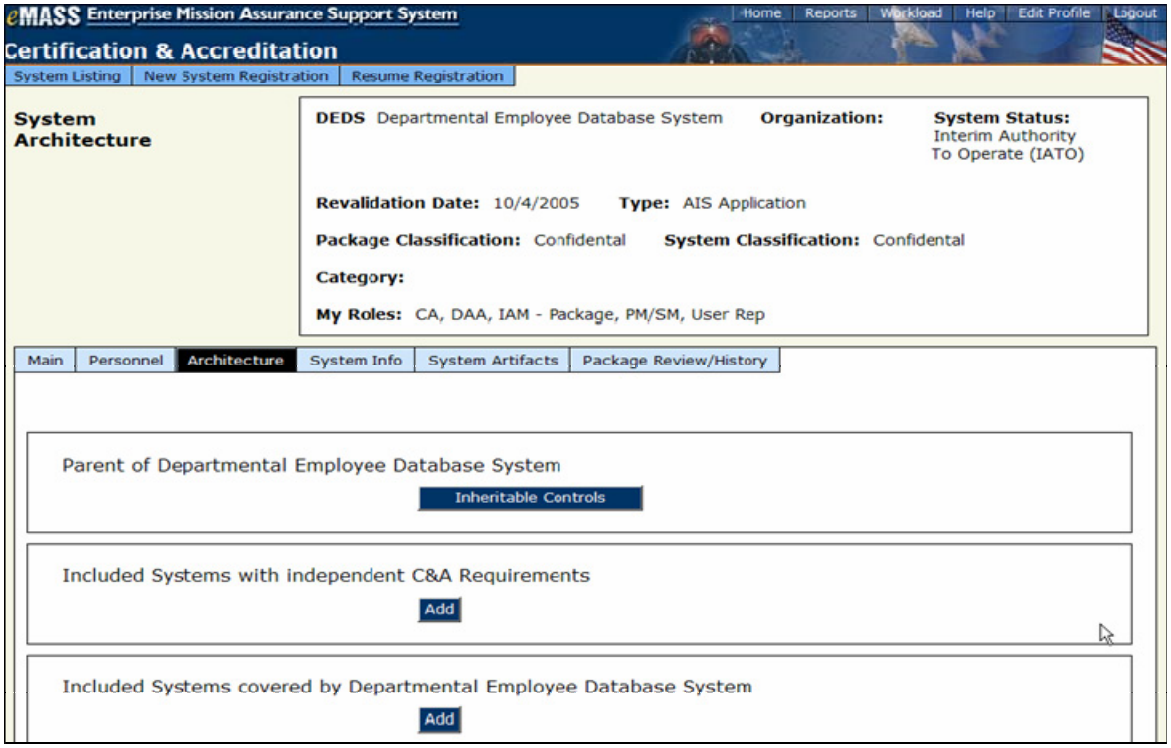


Figure 68. eMASS Certification and Accreditation (C&A) Entering System Architecture [From 16]

d. eMASS Reporting Module

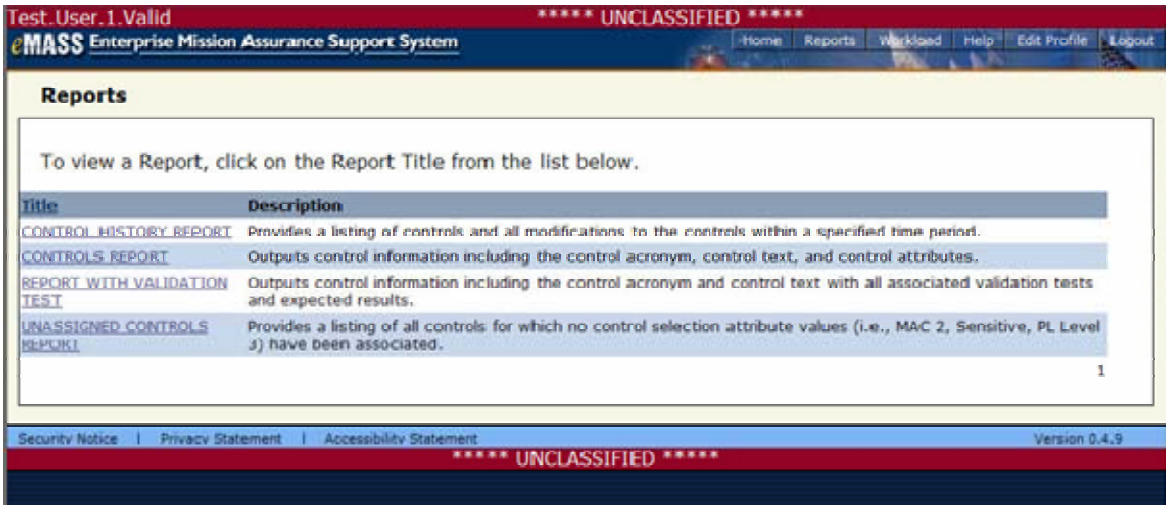


Figure 69. eMASS Generating Common Reports
[From 16]

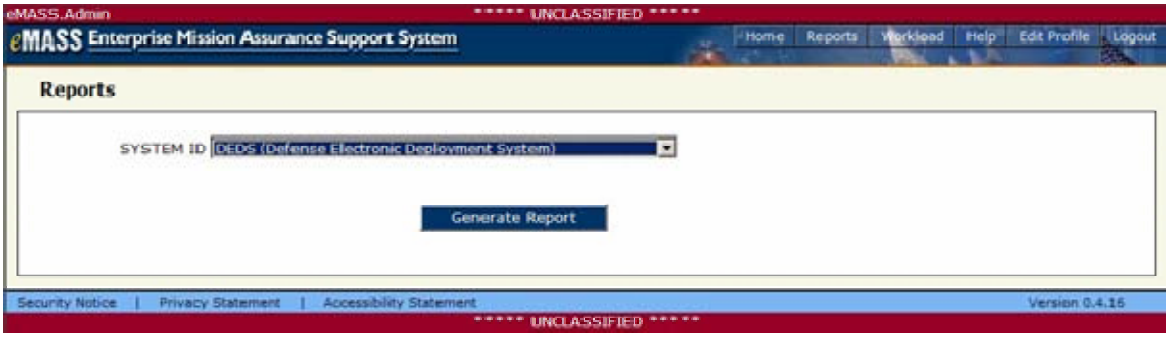
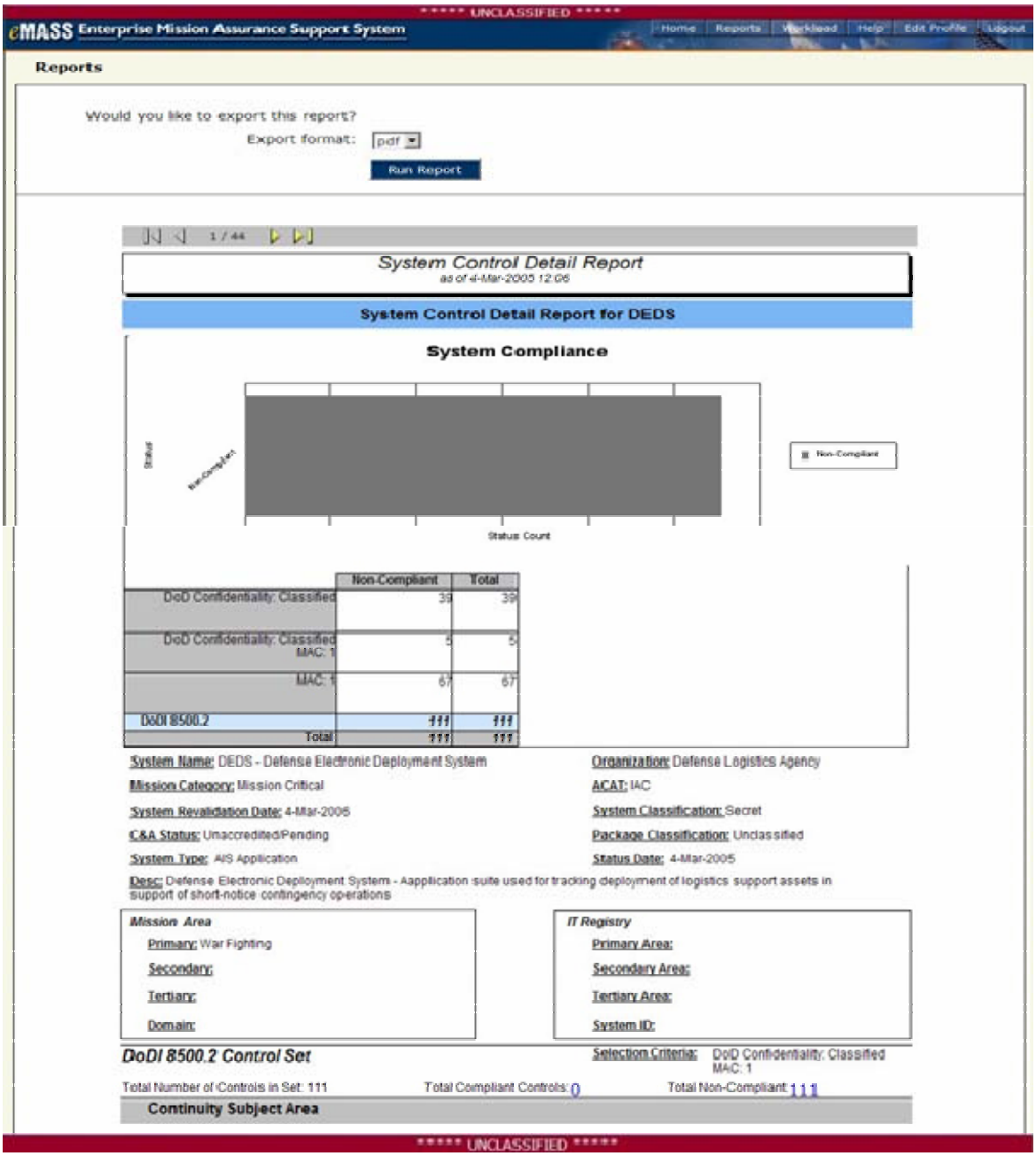


Figure 70. eMASS Report Customization
[From 16]



eMASS Report Customization (cont'd)
[From 16]

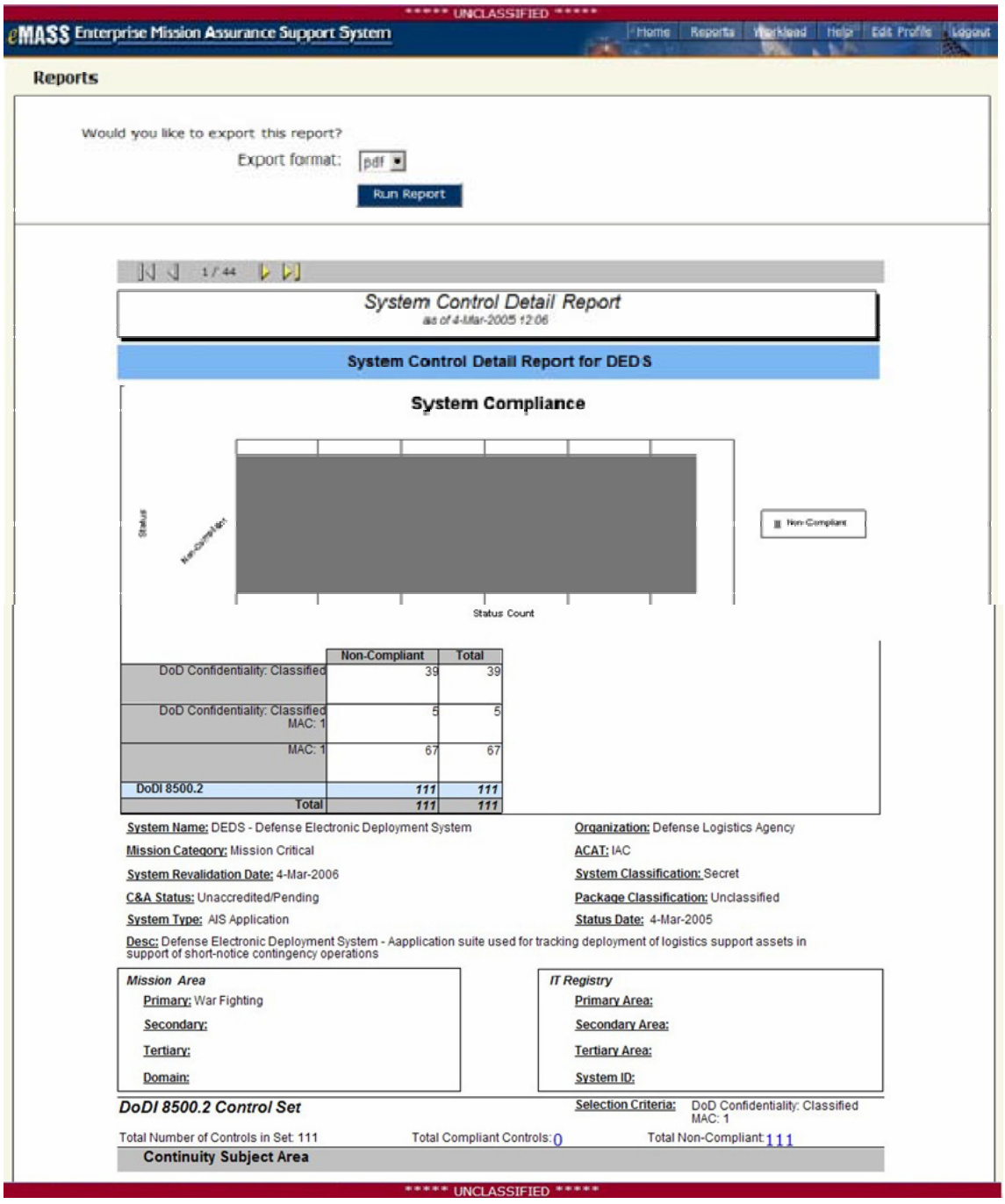


Figure 71. eMASS Report Customization Export
[From 16]

IV. RESEARCH FINDING AND ANALYSIS

A. INTRODUCTION

The key objectives of this analysis are to (1) describe exactly what capabilities and functionalities that the automated C&A tools provide to the main C&A proponents, especially assisting the DAA, in making an informed accreditation decision, and more importantly, (2) analyze and understand IA controls and use mapping techniques to demonstrate evidence that the IA controls were being satisfied regardless of the C&A process. The recognition of these objectives will reinforce the relationship of the standardized DoDI 8500.2 IA controls structure as a basis for IA C&A. This understanding will provide valuable insight to further expand the knowledge base of the Navy Medicine DAA in authorizing the operation of mission essential Navy Medicine health information systems and managing IA posture across Navy Medicine based on consistent IA controls.

The analysis for this study was done utilizing two methods. In the first method, a limited number of Navy Medicine IA staff, C&A Information Assurance personnel from SPAWAR San Diego and Charleston, and IA representatives from Telos Corporation and the Information Assurance Analysis Center were interviwed for this study. The selected individuals have considerable experience in the field of IA and are experienced users and developers of automated C&A tools. The interview for this study was conducted via phone and email. The questions on the interview focused on the IA posture of Navy Medicine C&A and information on the performance of the two automated C&A tools, namely, Xacta and eMASS. Afterwards, the results of the interview were collected, categorized and analyzed.

In the second method, two attachments from the DoDI 8500.2, Information Assurance Implementation Guide were used in the policy analysis. For the purpose of this analysis, these two attachments represented the recommended assurance levels and integrity, availability and confidentiality thresholds needed in the processing, handling and storage of protected health information (PHI) being transmitted across Navy Medicine information systems. The first attachment used was the E4.A2, Attachment 2 to

Enclosure 4, Mission Assurance Category II (MAC II) for High Integrity and Medium Availability and the second attachment was E4.A5, Attachment 5 to Enclosure 4 Confidentiality Controls for DOD Information Systems Processing Sensitive Information. The IA controls from the two attachments were mapped to the sections and appendices of the DITSCAP SSAA. The results of the mapping were tabulated and analyzed.

B. C&A AUTOMATED TOOL ANALYSIS

The limited information obtained describing the actual performance of the two C&A tools, Xacta and eMASS, were based on interviews from experienced users of the automated tools and review of literature from the developers of the automated tools.

1. Xacta C&A Automated Tool Analysis

Some of the observations that were provided by actual users of the Xacta C&A tool described it as a web-based tool that requires a license for each project. The tool requires a Structured Query Language (SQL) server on a host computer. The Xacta administrator creates and deletes user accounts and privileges and Xacta's output is in Microsoft Word (MS Word) format.

In actually using the Xacta C&A tool, the users described the advantages in utilizing the tool in completing the C&A projects. Some of the benefits identified are:

(1) Generates significant time savings in creating templates for the SSAA and associated appendices. The tool assists in formatting, table creation and publishing.
(2) Facilitates automatic creation of the Security Requirements Traceability Matrix (SRTM) and the Security Test and Evaluation (ST&E) Plan. The tool provides a user friendly interface for entry of ST&E results.
(3) Provides a guided method in evaluating residual risks with an automatic creation of the risk assessment documentation. The tool contains many built-in references and predefined summaries of the DITSCAP 8510.1-M sections.
(4) Provides a built-in vulnerability and scanning tool functionality.
(5) Provides flexibility in allowing changes to the certain Xacta code that facilitates creation of additional sections to the SSAA.
(6) Provides a customer-oriented, service based, excellent response time, technical and customer Xacta tool help desk support.

However, the users of the Xacta C&A tool also described some disadvantages they experienced in using the tool for their C&A projects. Some of the challenges are:

(1) There was difficulty in tracing the ST&E cases back to the SRTM. The ST&E plan created by the tool did not include a summary matrix with backward referencing. A manual trace on hardcopy SSAA has to be done by the SSAA reviewers.
(2) The presentation of results for the Detect Tool is not user friendly. The vulnerability information results should be improved to have a more user friendly format similar to the Internet Security Solutions System Scanner (ISS) format for ease on user familiarity.
(3) The vulnerability information results generated by the Xacta Detect tool were not automatically included in the residual risk assessment determination. There should be a feature that allows user options to include the vulnerability information in the risk assessment.
(4) The spell check feature was not available as a built in function in the Xacta tool. This functionality becomes accessible only after document generation in MS Word format. Spell checking the SSAA and appendices after publishing became an extra step and a time consuming task.
(5) The Appendix A generated by the Xacta C&A tool contained numerous outdated acronyms. Automatic addition of new acronyms to Appendix A should be a built-in feature. Considerable time and effort was needed to manually tailor Appendix H (Security Test and Evaluation Plan and Procedures) to the actual SSAA. This effort resulted in the reduction of the total number of appendix pages from 16 to 5 pages.

The observations noted by users of the Xacta C&A tool yielded suggested improvements for the IS developers. These suggested improvements include:

(1) The automatic generation of the ST&E document should include all the tests that are referenced in the SRTM. Otherwise, the Xacta tool must be able to inform the user if there were tests in the SRTM that were not included in the ST&E. This is a critical feature that can affect the tool's overall usability.
(2) An automated trace back functionality from the ST&E to the SRTM should be built in together with tabular or matrix format information that allows for a manual trace back. The automatic trace back is a useful tool for the Xacta C&A tool users and the manual trace back feature is for the reviewers using SSAA printed copies.
(3) The format of the Detect Tool vulnerability scan information should be modified to a format similar to the ISS vulnerability scan result format. This allows for ease of navigation and readability for the Xacta C&A tool users.

2. eMASS-NG C&A Automated Tool Analysis

The next generation eMASS C&A tool is on its final development stage and will be available through several pilots in the near future. However, one of the key things in the literature review provided by the developers of eMASS noted that the eMASS base code is the property of DoD. A quality that can be crucial in terms of cost benefit especially in software licensing. An analysis of the eMASS-NG functionalities and capabilities will be discussed based on the literature review obtained from the eMASS developers.

Unlike Xacta which is DITSCAP based, eMASS is based on a newly written IA process called the DoDI 8510.bb, Defense Information Assurance Certification and Accreditation Process (DIACAP). The DIACAP is a new process for the C&A of all DoD information systems and is projected to be the future replacement to DITSCAP pending review and approval from DoD and all its branch services.

At the core of eMASS is the DIACAP Knowledge Base (KB) also known as Knowledge Services (KS). The Knowledge Base is a web based DIACAP knowledge bank that provides current GIG IA C&A guidelines. It is a repository of tools, diagrams, process maps, artifacts to assist and facilitate in DIACAP execution. More importantly, it gathers members of the C&A user working group to collaborate by developing, trading and sharing best business lessons and practices discovered in the C&A process. The KB also serves as source of IA current events keeping users updated with pertinent IA information.

For the purpose of IA, DIACAP classifies all DoD IS into four main categories. The categories are (1) enclaves, (2) AIS applications, (3) outsourced IT-based processes and (4) platform IT interconnections. The importance of the DIACAP process in support of a manual or automated C&A process is it allows (1) the users to relentlessly supervise IA systems to ensure conformity with key regulatory, like DoD 8500 series and legislative, such as FISMA policy, (2) the data from all IA systems to be electronically documented, (3) determines limits or boundaries and (4) IA systems achieve C&A conforming to policy standards.

A KB user can expect to find the KB as one stop shop that would facilitate the C&A process by assisting the user in (1) discovering the most updated GIG IA C&A guidelines, (2) achieving the proper control set identification in a system, (3) acquiring validation tests and its established results, (4) getting and sharing global advice from fellow IA users implementing the DIACAP process, (5) accessing useful publishing tools and (6) obtaining the most current reliable information on software testing tools.

The method eMASS maps to the C&A policy is by managing the key activities in the DIACAP workflow and by automatically producing the C&A process workflow when a system is registered, personnel chosen to enforce the process functions and a system C&A package is produced.

The role of the C&A proponents in eMASS are aligned to the C&A policy. Some of the default C&A roles in eMASS are the Designated Approving Authority (DAA), Certification Authority (CA), Program Manager (PM), User Representative (UR), Information Assurance Manager (IAM), Validation Tester and eMASS Administrator. The combination of role and organization determine user authority in accessing different components of eMASS. Personnel assigned to these roles perform critical functions in the C&A workflow. Additional new roles can be configured as needed. Section 6.5 of the DITSCAP identify and define the C&A team members responsible for the development of the SSAA however, the eMASS Assign Personnel feature in the C&A module assists the user in determining the names of the C&A team members assigned to the C&A roles.

One of the key features of eMASS is its Controls Administration Module (CAM). The eMASS CAM allows its users to author and manage IA control sets, subject areas and controls appropriate to three layers. These layers are the DoD Enterprise, DoD Component, and DoD Information System. The CAM allows users to attach implementation guidance to IA controls as reference material while performing the C&A. This is very useful especially when C&A reviewers want to do a trace back. The CAM also provides users with the ability to author generic validation procedures and expected results for IA controls. Lastly, the eMASS CAM permit users to generate controls reports to determine residual risk on sections that warrant remediation. The eMASS CAM is also responsible for the handling of IA controls MAC and Confidentiality. Through the

eMASS CAM suggested ways of implementing activities required to achieve the implementation of IA controls can be assigned and accounted.

The eMASS C&A module authorize users to (1) view systems within eMASS where the user has appropriate level access, (2) enroll new systems using the IT registration procedure, (3) oversee and handle IA controls and their respective validation procedures, and (4) interface with systems as the workflow process is accomplished.

The concept of inheritability is implemented as a time saving feature in the eMASS C&A module. This concept of inheritability allows the use of a system's control status and applying it to another system much like a parent to a child. These parent and child relationship between systems can be established during the eMASS registration process. Users can save time by using the inheritability characteristic in the eMASS C&A module by applying a parent's system's control status and validation test results. This means that if a child system package inherits control status from its parent system package for one of its controls then the user does not have to test that control and the parent system's test result would count for the child system package. This eliminates redundancy and saves time.

The concept of acceptance is also implemented in the eMASS C&A module. This time this concept allows parent systems to accept child system tests for a control for independent included system only. This comes very useful only for IA controls of a similar grouping. However, controls must be of equal or greater stringency on the child system.

The next generation eMASS C&A tool will be made available to its users without charge for licensing or development upgrades. eMASS also claims that it does not require an organizational investment in COTS software licenses and training (eMASS-NG, 2004). The eMASS free licensing feature may prove to be beneficial in total cost of ownership compared to the licensing issues that affected the Xacta users.

C. INFORMATION ASSURANCE POLICY ANALYSIS

The information obtained in the analysis of IA policy was conducted using the DODI 8500.2 and the DITSCAP SSAA. The DODI 8500.2 enforces policy, designate

responsibilities and stipulate procedures for administering integrated, layered protection the DoD information systems and networks as prescribed in the DoD Directive 8500.1. The DODI 8500.2 ensures that information assurance levels for DoD information systems are assigned explicit IA controls. DODI 8500.2 is a major instruction that is strictly followed for compliance by all automated C&A tool vendors and developers. The SSAA is the cornerstone document of the DITSCAP that captures all of the IA controls for a system. The SSAA also discusses IA control implementation in the architecture and design and pretests the test procedures for testing the controls.

With the advent of the Health Insurance Portability and Accountability Act (HIPAA) Final Rule on Security and Privacy, it was assumed, for the purpose of this analysis, that the highest possible data classification for Navy Medicine healthcare information was a Mission Assurance Category II (MAC II) High Integrity and Medium Availability level and a Sensitive Information Confidentiality Control level. Each IA control from the specified sections of the DODI 8500.2 was mapped to each DITSCAP SSAA section. The purpose of this analysis is to show that the IA controls required in DODI 8500.2, as applied to Navy Medicine healthcare data, have a proper place for discussion and consideration in the DITSCAP SSAA.

The mapping of the DODI 8500.2 IA controls against the DITSCAP SSAA sections resulted in two tables. The tables showed the IA Control Number, IA Name, IA Service and the corresponding SSAA paragraph number(s) that map to the specific IA control. After completing the tables, each SSAA appendix and section number was verified with its mapping to an IA control. The results showed that all the SSAA sections mapped to the IA controls with the exception of three sections in the DITSCAP SSAA.

This result shows that certain sections of the SSAA that did not map to an IA control may (1) have no purpose, (2) be used as an introduction for a more detailed section, (3) be extraneous, or (4) be a section with duplicate information and can be discarded. Sections of the SSAA that did not map to the IA controls can be removed from the SSAA. This can result to a more concise, shorter format of the SSAA. However, these sections have to be carefully examined in context. Sections of the SSAA that exist for readability for the C&A proponents can remain in the SSAA.

The three SSAA sections that did not map to any IA control are shown in Table 7. After careful examination of the description of each section it became obvious that these sections exist in the SSAA for the purpose of readability, clarity and tractability.

The Certification and Accreditation Statements (Appendix R) did not map to any IA control but are in the SSAA because they are simple paragraphs where the Certifier attests that the system meets the design and implementation standard per regulation and policy, that the system complied with the defined security requirements operating the system and that the DAA approves of the risk to the system as designed, giving an approval to operate (ATO) or interim approval to operate (IATO). This appendix can be condensed into a single document but it is a necessary document in the SSAA.

The Acronym List (Appendix A) did not map to any IA control but is necessary in the SSAA because it facilitates clarity in describing the user's information system certification and accreditation documentation. Users should develop their own list of appropriate acronyms that are tailored for their C&A process.

Section 2.1 of the SSAA, Operating Environment did not map to any IA control but is still necessary documentation in the SSAA because it provides an overview of the operating environment. It serves as an introductory section for readability and prepares the section for a detailed analysis of the Operating Environment in the subsections. The set of IA controls that were used for this analysis required mappings to detailed sections of the SSAA. That accounted for subsections of Section 2.1, (Facility Description, Physical Security, Administrative Issues, Personnel, COMSEC, TEMPEST, Maintenance Procedures, and Training Plans) to map to the IA controls and not Section 2.1, which provided an overview of the operating environment section of the system.

Table 6. Mission Assurance Category (MAC) II for High Integrity and Medium Availability
E4.A2 Attachment 2 to Enclosure 4
IA Control Mapping to DITSCAP SSAA

IA Control Number	IA name	IA services	SSAA paragraph. No.
DCAR-1	Procedural Review	Availability	4.1;4.4;4.7;Appendix L
DCBP-1	Best Security Practices	Integrity	4.4;4.5; 6.1.3;
DCCB-2	Control Board	Integrity	2.2;4.4;4.6
DCCS-2	Configuration Specifications	Integrity	4.4;4.5; Appendix M; Appendix C
DCCT-1	Compliance Testing	Availability	Appendix G; Appendix H
DCDS-1	Dedicated IA Services	Integrity	1.3.2; 2.1.4; 2.1.5; 2.1.7;4.3; 5.4; Appendix Q; Appendix F
DCFA-1	Functional Architecture for AIS applications	Integrity	1.1; 1.2; 1.3.4; 2.1.4; 2.1.5; 3.1;3.2;3.3;4.3; Appendix L, Appendix M
DCHW-1	Hardware Baseline	Availability	3.1;
DCID-1	Interconnection Documentation	Integrity	1.1; 3.2; 4.5; Appendix N
DCII-1	IA Impact Assessment	Integrity	4.7;
DCIT-1	IA for IT Services	Integrity	2.1.4; 2.1.5; 2.1.6; 2.1.7; 4.3;
DCMC-1	Mobile Code	Integrity	4.1; 4.2; 4.4; 6.1.1; Appendix Q;
DCNR-1	Non-Repudiation	Integrity	2.1.5; 4.4
DCPA-1	Partitioning the Application	Integrity	3.1; 4.4;
DCPB-1	IA Program and Budget	Availability	5.2; 6.2; 6.3; 6.4
DCPD-1	Public Domain Software Controls	Availability	2.2; 3.1; 3.2; 4.4; Appendix Q
DCPP-1	Ports, Protocols, and Services	Availability	1.3.1; 2.1.5; 3.1; 3.2; 3.3
DCPR-1	CM Process	Integrity	4.6; 4.7; Appendix G; Appendix H
DCSD-1	IA Documentation	Availability	1.3.4; 5.1; 5.3; 6.2; 6.3; 6.5; Appendix C; Appendix E;
DCSL-1	System Library Management Controls	Integrity	2.2; 3.1; 3.3; 4.4
DCSP-1	Security Support Structure Partitioning	Integrity	3.1; 3.2; 4.4;
DCSQ-1	Software Quality	Integrity	1.3.5; 2.2; 3.1; Appendix H; Appendix B; Appendix P
DCSS-2	System State Changes	Integrity	1.3.1; 2.1.7; Appendix H, P
DCSW-1	SW Baseline	Availability	2.1.7;3.1; Appendix L
IAKM-2	Key Management	Integrity	2.1.5;

IATS-2	Token and Certificate Standards	Integrity	2.1.5;
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	Integrity	1.3.1; 2.1.3; 2.1.7; 3.1; Appendix J
ECCD-2	Changes to Data	Integrity	1.3.3; 1.3.4; 2.1.3; 4.7; Appendix M
ECDC-1	Data Change Controls	Integrity	2.1.3; Appendix J
ECID-1	Host Based IDS	Integrity	1.4; 2.1.5; 3.1; 3.2; 3.4
ECIM-1	Instant Messaging	Integrity	2.1.5; 3.2; 4.4; 4.5;
ECND-2	Network Device Controls	Integrity	2.1.3; 2.1.7; 2.2; 3.2; Appendix J
ECPA-1	Privileged Account Control	Integrity	1.3.4; 2.1.4; 6.1.2
ECPC-2	Production Code Change Controls	Integrity	1.3.4; 2.1.3; 2.1.4; Appendix J
ECRG-1	Audit Reduction and Report Generation	Integrity	1.3.1; 2.1.3; 2.1.7; 3.1; Appendix J
ECSC-1	Security Configuration Compliance	Availability	4.1; 4.2
ECSD-2	Software Development Change Controls	Integrity	1.3.4; 2.2;
ECTB-1	Audit Trail Backup	Integrity	1.3.1; 2.1.3; 2.1.7; 3.1; Appendix J, Appendix M
ECTM-2	Transmission Integrity Controls	Integrity	2.1.5; 2.1.6; 3.2; 3.3; 4.5; Appendix M
ECTP-1	Audit Trail Protection	Integrity	2.1.3; 2.1.7; Appendix J
ECVI-1	Voice over IP	Availability	2.1.5; 3.2; 4.5
ECVP-1	Virus Protection	Availability	2.1.7; 3.2; 4.4; 6.1.4 Appendix J; Appendix M; Appendix Q;
ECWN-1	Wireless Computing and Networking	Availability	2.1.5; 3.2; 4.4; 4.5; Appendix C
EBCR-1	Connection Rules	Availability	2.1.5; 3.2; 4.1; 4.2; 4.5
EBVC-1	VPN Controls	Availability	1.4; 2.1.5; 3.1; 3.2; 3.4
PEEL-2	Emergency Lighting	Availability	2.1.1;2.3; 4.4; Appendix K
PEFD-2	Fire Detection	Availability	2.1.1; 2.1.2; 2.3; 4.4; Appendix K
PEFI-1	Fire Inspection	Availability	2.1.1; 2.1.2; 2.3; 4.4; Appendix L
PEFS-2	Fire Suppression System	Availability	2.1.1; 2.1.2; 2.3; 4.4; Appendix K
PEHC-2	Humidity Controls	Availability	2.1.1; 4.4; 2.3; Appendix K
PEMS-1	Master Power Switch	Availability	2.1.2; 4.4; Appendix K

PESL-1	Screen Lock	Integrity	2.1.2; 4.4; Appendix K
PETC-2	Temperature Controls	Availability	2.1.2; 4.4; 2.3; Appendix K
PETN-1	Environmental Control Training	Availability	2.1.2; 2.1.4; 2.1.8; 4.4; Appendix M; Appendix O
PEVR-1	Voltage Regulators	Availability	2.1.2; 4.4;
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	Availability	2.1.3; 2.1.4; Appendix J
COAS-2	Alternate Site Designation	Availability	2.1.1; Appendix E, J
COBR-1	Protection of Backup and Restoration Assets	Availability	1.3.1; 2.1.3; 2.1.7; 3.1; 4.3; Appendix J, M
CODB-2	Data Back-up Procedures	Availability	1.3.1; 2.1.3; 2.1.7; 3.1; 4.3; Appendix J, M
CODP-2	Disaster and Recovery Planning	Availability	2.1.7; Appendix D; K; L;
COEB-1	Enclave Boundary Defense	Availability	2.1.1; 3.4; 4.4; Appendix L
COED-1	Scheduled Exercises and Drills	Availability	1.3.4; 2.1.4; 2.1.8; Appendix K, L
COEF-2	Identification of Essential Functions	Availability	1.3.4; 2.1.3; 2.1.7; Appendix J
COMS-2	Maintenance Support	Availability	2.1.7; 4.4; Appendix E
COPS-2	Power Supply	Availability	2.1.7; 4.4; Appendix E
COSP-1	Spares and Parts	Availability	2.1.7; 4.4; Appendix E
COSW-1	Backup Copies of Critical SW	Availability	1.3.1; 2.1.3; 2.1.7; 3.1; Appendix J, Appendix M
COTR-1	Trusted Recovery	Availability	2.1.3; 2.1.7; 4.4 Appendix E; Appendix H; Appendix J; Appendix L
VIIR-1	Incident Response Planning	Availability	2.1.8; 5.4; Appendix K; Appendix O
VIVM-1	Vulnerability Management	Availability	2.1.8; 4.4; 4.6; Appendix E; Appendix O

Table 7. Confidentiality Controls for DOD Information Systems Processing Sensitive Information
E4.A5 Attachment 5 to Enclosure 4
IA Control Mapping to DITSCAP SSAA

IA Control Number	IA name	IA services	SSAA paragraph. No.
DCAS-1	Acquisition Standards	Confidentiality	1.3.1; 1.3.2; 1.3.5; 3.1; 3.2; 4.4; 6.1.1; 6.1.4; Appendix D, Appendix E, Appendix I
DCSR-2	Specified Robustness - Medium	Confidentiality	1.3.1; 1.3.2; 3.1; 3.2; 4.3; 4.4; Appendix D, Appendix E
IAGA-1	Group Identification and Authentication	Confidentiality	1.3.4; 2.1.5; 6.5; Appendix M
IAIA-1	Individual Identification and Authentication	Confidentiality	1.3.1; 1.3.4; 2.1.2; 2.1.7; 6.1.3; Appendix H
ECAD-1	Affiliation Display	Confidentiality	1.3.1; 1.3.4; 4.4; Appendix E, Appendix H
ECAN-1	Access for Need-to-Know	Confidentiality	1.3; 1.3.3; 1.3.4; 2.1.3; 3.3; 4.4; 4.5; Appendix J
ECAR-2	Audit Record Content	Confidentiality	2.1.3; 4.4; 4.5; 6.1.2
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	Integrity	2.1.3; 4.4; 4.5; 4.7; Appendix B; Appendix C; Appendix F; Appendix Q
ECCR-1	Encryption for Confidentiality (Data at Rest)	Confidentiality	2.1.5; 4.3;
ECCT-1	Encryption for Confidentiality (Data in Transit)	Confidentiality	2.1.5; 3.2; 3.3; 4.3; 4.5; 6.1.3;
ECIC-1	Interconnections among DoD Systems and Enclaves	Confidentiality	3.2; 4.5; Appendix N
ECLO-1	Logon	Confidentiality	1.3.4; 2.1.4; 2.1.7; 2.2; 4.5;
ECLP-1	Least Privilege	Confidentiality	1.3.4; 2.1.4; 2.2; 4.5; 6.1.2

ECML-1	Marking and Labeling	Confidentiality	1.3.3; 3.1; 3.2; 4.3;
ECMT-1	Conformance Monitoring and Testing	Confidentiality	2.3; 4.6; 6.2; 6.3; Appendix G; Appendix H, Appendix P; Appendix Q
ECNK-1	Encryption for Need-To-Know	Confidentiality	1.2; 1.3.3; 1.3.4; 3.3; 4.3;
ECRC-1	Resource Control	Confidentiality	1.3.1; 2.1.7; 2.3
ECRR-1	Audit Record Retention	Integrity	2.1.3; 4.4; 4.5; Appendix Q
ECTC-1	Tempest Controls	Confidentiality	2.1.6; Appendix M
ECWM-1	Warning Message	Confidentiality	1.1; 2.1.3; 3.1; 4.1; 4.2; 4.4; Appendix C; Appendix J, Appendix M
IAAC-1	Account Control	Confidentiality	1.3.4;2.1.3; 4.4; Appendix M
EBBD-2	Boundary Defense	Confidentiality	1.2; 3.1; 3.2; 3.4; 4.2; 4.5;
EBPW-1	Public WAN Connection	Confidentiality	3.1; 3.2; 4.2; 4.5; Appendix N
EBRP-1	Remote Access for Privileged Functions	Confidentiality	1.4; 1.3.4; 2.1.3; 3.1; 3.2; 4.5; Appendix E, Appendix F; Appendix J
EBRU-1	Remote Access for User Functions	Confidentiality	1.4; 1.3.4; 2.1.5; 3.1; 3.2; 4.5; Appendix E, Appendix J
PECF-1	Access to Computing Facilities	Confidentiality	2.1.2; 2.1.5; 2.1.7; 4.4; Appendix E, Appendix M
PECS-1	Clearing and Sanitizing	Confidentiality	3.1; 4.3;
PEDI-1	Data Interception	Confidentiality	1.3.3; 1.3.4; 2.1.2; 3.1; 4.3;
PEPF-1	Physical Protection of Facilities	Confidentiality	2.1.2; 2.1.5; 2.1.7; 4.4; Appendix E, Appendix M
PEPS-1	Physical Security Testing	Confidentiality	2.1.1; 2.1.2; 2.1.3; 2.1.7; Appendix J, Appendix H
PESP-1	Workplace Security Procedures	Confidentiality	2.1.1; 2.1.2; 2.1.4; Appendix E, Appendix M

PESS-1	Storage	Confidentiality	2.1.1; 4.3; Appendix E, Appendix M
PEVC-1	Visitor Control to Computing Facilities	Confidentiality	2.1.2; 2.1.3; 2.1.4; Appendix E, Appendix M
PRAS-1	Access to Information	Confidentiality	2.1.2; 2.1.4; 2.1.7; 2.2; Appendix E, Appendix M
PRMP-1	Maintenance Personnel	Confidentiality	2.1.4; 2.1.7; 4.4; Appendix M
PRNK-1	Access to Need-to-Know Information	Confidentiality	1.3.4; 2.1.4; 3.3; 4.4; 5.2; Appendix E, Appendix M
PRTN-1	Information Assurance Training	Confidentiality	2.1.8; 4.4; 5.1; 5.3; 5.4; 6.5; Appendix E; Appendix K; Appendix L; Appendix O

Table 8. Mapping Analysis of IA Controls to SSAA
For MAC II High Integrity and Medium Availability and
Confidentiality Controls for DoD Processing Sensitive Information

SSAA Section	Section Name and Description	Comments
Appendix R	Certification and Accreditation Statements Purpose: This appendix contains the formal authorization statements issued by the CA and DAA for the system to operate and supporting accreditation documentation. Provide copies of: • Requests for DAA Approval from the Program Office • Endorsement Letters from the Certification Authority • DAA Letters of Approval/Accreditation - Approval to Proceed - Interim Approval to	These C&A Statements provide readability and proof that the DAA approves of the risk to the system as designed, giving an approval to operate (ATO) or interim approval to operate (IATO).

	Operate - Approval to Operate.	
Appendix A	Acronym List	This is used as reference document for clarity.
Section 2.1	OPERATING ENVIRONMENT Purpose: This paragraph details the physical environment in which the system will operate, including the description of the facilities, physical security, administrative issues and personnel security. Contents Provide a generic description of the requirements for the physical environment in which the system will operate, including: • The facility • Physical and administrative security features • Maintenance procedures	Serves as an introductory section. The Subsections of Section 2.1 were specifically referenced more due to the detailed nature of the IA controls for MAC II High Integrity and Medium Availability and the Sensitive Confidentiality of the processed information as stated in DODI 8500.2. This section provides readability to the SSAA.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

A. INTRODUCTION

The C&A process within the DoD, MHS and Navy Medicine is achieved in accordance with DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)." It enforces the IA policies described in DoDD 8500.1, "Information Assurance (IA) and DoDI 8500.2, "Information Assurance (IA) Implementation". The DITSCAP applies to all the elements of the DoD, their contractors and agents. Furthermore, it is adopted by milestone decision authorities when acquiring IT resources and for the acquisition, administration and sustainment of any DoD system that is in the business of collection, storage, transmission or handling of unclassified, sensitive but unclassified or classified information.

The MHS IA Policy/Guidance and the BUMED AIS Security Program Policy is the governing policy for all Navy Medicine C&A initiatives. Policy is a major vector of IA vulnerabilities in large and complex organizations. Automated C&A tools that have a formal policy analysis methodology based on knowledge management tools, particularly object oriented databases, can greatly reduce policy-based vulnerabilities. Automated C&A tools like Xacta and eMASS have to comply with major federal, DoD and civilian IA and C&A policies. These tools must have enough flexibility to accommodate future policies and policy changes. Automated tools, if designed properly, have the potential to provide standardized C&A security across sites and systems with web based workflow and configuration management. These automated C&A solutions can (1) reduce required resources, (2) improve C&A process turn around time (3) ensure consistent standards, (4) provide accurate and comprehensive management reporting for the enterprise, (5) be scaleable. These tools can greatly enhance the information needed by a DAA in making a sound and well founded decision in either accepting or rejecting the residual risk assessment to allow an ATO or IATO.

B. THESIS QUESTIONS REVIEW

1. Are existing Navy Medicine C&A policies in alignment with current DoD, Navy Policy and federal government requirements? The existing Navy Medicine C&A policy is accomplished in accordance to the BUMED AIS Security Program Policy Manual and the MHS IA Security Policy/Guidance Manual version 1.3. The BUMED and MHS IA Security manuals strictly conform to the DoDI 5200.40, DoDD 8500.1 and DoDI 8500.2. However, Navy Medicine C&A policies would need to be updated to reflect relevant changes in the current policy that may be a result of the use of automated C&A tools in the C&A process.

2. Would the use of automated C&A software technology benefit the Navy Medicine C&A process? The use of automated C&A software technology would benefit Navy Medicine C&A process. This is true provided that Navy Medicine C&A team invest time and resources in evaluating the right tool that would fit the Navy Medicine C&A process. The Navy Medicine C&A process follow the DITSCAP. Navy Medicine commands and activities still use the manual method of C&A. Information gathering entails manual entry of hardware and software information. The management of security regulations are done by manually highlighting applicable regulations in hard copy or softcopy of IA security manuals. Testing is accomplished by manual development of checklists and test procedures. Document formatting is produced by using multiple word processing applications, managing fonts, tabs, formats and the like. The use of automated C&A tools like Xacta and eMASS can greatly improve the quality and turn around time of the C&A reporting and documentation in the Navy Medicine C&A process.

3. Would the use of automated certification and accreditation tools be a cost effective means to address Navy Medicine C&A IA threats and vulnerabilities? Historical data showed that Navy Medicine has approximately 15,000 health and patient care related systems including legacy systems. It approximately costs Navy Medicine around $2M per year in maintenance costs to protect its information assets using manual scanning and patch management alone as part of compliance to the Navy Medicine C&A and HIPAA requirements. The Xacta Group estimates that for a Level 3 C&A or equivalent (DITSCAP, NIACAP, NIST, DCID), a local area network with 250 devices consisting of 50 servers, routers and switches, including 200 workstations and printers

with platforms ranging from Windows, HPUX, Linux and Solaris, at $80.00 per hour the total cost of a C&A project for a system using the manual C&A method would cost an estimated $180,480 using an estimated 2,256 man hours. But by using the Xacta C&A tool with its automated C&A features, the C&A process of a similar system would be completed with an estimated reduced cost of $52,640 using 658 man hours. The organization can have considerable savings using automated C&A tools in their C&A process.

The functionalities of automated C&A tools can greatly improve the manual Navy Medicine C&A process by its (1) automatic discovery, inventory, scanning and loading of C&A information in its central database, (2) automatic generation of the SRTM , (3) automatic generation of content management documentation, (4) automatic mapping to test procedures to determine pass or fail conditions, and (5) automatic publishing capabilities for the SSAA and its appendices.

The use of automated C&A tools would not replace the Navy Medicine C&A staff but it would allow them valuable time to address other significant IA and C&A issues. The automated C&A software technology would prove beneficial especially if Navy Medicine has the means of acquiring them like the Xacta C&A tool. In addition, eMASS can prove to be very beneficial automated C&A solution for Navy Medicine especially because it is owned by DoD and will be made available without charge for licensing or development upgrades.

4. Would a consolidated and centrally-managed knowledgebase of C&A policies improve Navy Medicine's current security posture?

The automated C&A tools, Xacta and eMASS, were designed with the core of their content management functionality stored in centrally managed databases. The Xacta IA Manager Enterprise edition has an internal relational knowledge base and database that stores over 100 leading federal, DoD, and civilian regulations and policies for IT risk compliance and management. The eMASS-NG also has an integrated knowledge base resource that provides current Global Information Grid (GIG) C&A federal, DoD and civilian guidelines. It has a library of tools, diagrams, process maps, artifacts to support and aid in the execution of the C&A process.

These centrally managed knowledge base resources that are built in the automated C&A tools can revolutionize the Navy Medicine C&A process in effectively meeting their C&A objectives, proactively managing its IA program, and have real time decision support capabilities using one-time data entry to assist the DAA in making a sound decision of accepting or rejecting the residual risk assessment to approve, interim approve or reject system operation.

C. RECOMMENDATIONS FOR IMPROVING NAVAL MEDICINE CERTIFICATION AND ACCREDITATION PROCESS

This study looked into the role of automated C&A tools in the Navy Medicine C&A process by examining the capabilities of Xacta IA Manager and eMASS. It also looked into DoDI 8500.2 as a major DoD IA instruction as its IA controls are mapped to the DITSCAP SSAA.

In order for the Navy Medicine C&A process to fully benefit from using automated C&A tools, it has to examine if the automated C&A tool's functionalities fit their needs, match their resources and capabilities and add value to their C&A process. The mission of these C&A tools is to assist the C&A main proponents in establishing a C&A process that reduces required resources, ensures consistent standards, provides management reporting to the enterprise and is scaleable.

Given that the automated tools produce documentation that assists the DAA understand the residual risk, these tools should produce concise yet comprehensive and understandable reports to guide the DAA in making his decision. The Xacta IA Manager DITSCAP based tool produces the SSAA that provides the DAA with a complete report on the technical and non-technical information with test procedures to support the residual risk assessment. The SSAA which is a living document that (1) contains agreed items by the C&A main proponents and (2) identifies all costs relevant to the C&A process, is perceived to be a very tedious and time consuming document to complete.

On the other hand, eMASS, whose reporting format is still in development, is designing a more concise yet comprehensive score card which would assist the DAA in evaluating the residual risk assessment. eMASS is based on the Defense Information Assurance Certification and Accreditation Process (DIACAP) DoDI 8510.bb which is

projected to replace the DITSCAP once it passes evaluation by DoD and other federal agencies. Some suggested items that a DAA would like to see in the eMASS scorecard would be a report that shows evidence of the risk such as a concise residual risk scorecard that documents the technical risks discovered in the C&A process with the associated management impacts with cost values in a prioritized list.

The Navy Medicine C&A team should closely scrutinize the internal and external capabilities of the automated C&A tools Xacta and eMASS. They need to consider how these tools can significantly contribute to the C&A process with its time-saving and value added features. Based on the analysis conducted on the two automated tools, below is a checklist containing suggested fact finding questions that would be the criteria in assisting Navy Medicine in evaluating the acquisition of an automated C&A tool.

Table 9. Criteria for selecting an appropriate automated C&A tool

Criteria	Yes	No
Does the automated C&A tool have a built in feature to handle IA control implementation and testing? Does the tool allow users to obtain suggested ways to implement and test IA controls or do the automated tools only produce an outline of technical information to assist the user in testing and implementing IA controls?		
Does the automated C&A tool create a collaborative workspace environment for its user community in order to develop, share and post lessons learned with best corrective actions? Does it provide a forum to hear about user real-world experiences implementing their chosen C&A policies?		
Does the tool automatically figure out what IA control sets are needed in a given system? Automatically find validation tests with expected test results?		
Is the tool web based? Is it publisher friendly? Does it allow easy access to useful forms and templates? Does it accept all standard characters? Does it allow the easy addition of extra sections in the report by modifying source code? Does it allow collaboration among multiple users or multiple roles?		
Does the tool interface with third party software testing tool like the Defense Information Systems Agency (DISA) Gold Disk? Does the tool generate test scripts for testing requirements? Does the tool have a built in vulnerability scanner?		

Does the tool have a steep or manageable learning curve? Is there 24/7 online or phone technical support for the users?		
Does the tool track the progress of IA activities? Does the tool track current C&A status of systems? Does the tool provide visibility into current IA system security status?		
Is the automated C&A tool cross compatible with different IA policies? Does it leave room for growth to accommodate new and revised policies?		
Does the tool's built in report generation feature allow customization of reports according to the role of the C&A proponent requesting the report? Does the automated C&A tool produce a report specific for the DAA, CA, PM, UR, IAM to assist them in their decision making or recommendation of an ATO or IATO of a system?		
Is the enterprise license for the tool free or proprietary? How much organizational investment in hardware, licenses and training is needed?		

D. SUMMARY

In summary, the analysis conducted in this research showed clear evidence that both automated C&A tools support the C&A process. The analysis of the automated C&A tools showed that the tools supported the proposed C&A process by mapping the confidentiality, integrity and availability assurance requirements following the DITSCAP. By taking the confidentiality, integrity and availability requirements of a typical naval healthcare system and mapping it to the DITSCAP, the analysis assured that the information assurance controls are confirmed in the information system or the network. Furthermore it assures the users that the cornerstone of the DITSCAP is definitively documented in the SSAA. The Xacta automated C&A tool using the DITSCAP showed that the C&A process was supported. The eMASS automated C&A tool provides suggested ways to incorporate the C&A documentation but does not directly do it for the users.

The benefit that can be derived from the utilization of automated C&A tools in the Navy Medicine C&A process can only promote a healthier, robust and more secure networking environment for Navy Medicine professionals while significantly decreasing residual risk. The constant increase of threats and vulnerabilities to systems in

conjunction with increased dependability on networked information systems, develop an overwhelming demand to maintain confidentiality, integrity and availability of information assets. The reduction of demand for resources required to conduct a C&A of a system using automated C&A tool will produce an immediate return on investment to Navy Medicine if funding allows for it. In purchasing an automated C&A tool, a good understanding of the C&A tool's expected functionality and features by the C&A team would prevent acquiring the wrong C&A tool resulting in wasted effort, money and man hours. Otherwise, the Navy Medicine C&A team should consider making plans to obtain and evaluate free government-off-the-shelf (GOTS) automated C&A tool to improve their C&A process.

Information assurance experts all over the world agree that today's networked domains are susceptible to more risk than before. Federal agencies, DoD components and civilian organizations that do not take advantage of the benefits of an automated C&A solution in combination with layered defenses expose themselves and their clients to an increased risk compared to those organizations that are continuously improving their IA security posture by being more proactive and assertive in securing their information system resources. By using an automated tool, an organization will facilitate capturing a detailed explanation of the implementation of the IA controls and development through test cases to confirm them. This will illustrate areas for risk management and more accurately represent the residual risk to the DAA for acceptance.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] DoD 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), Application Manual," July 2000

[2] DoD Directive 8500.1 "Information Assurance (IA)," October 2002

[3] DoD Instruction 8500.2 "Information Assurance (IA) Implementation," February 2003

[4] DoD 8510.bb, "Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)," September 2004

[5] DoD 5200.40, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 1999

[6] CJCSM 6510.01, "Chairman Joint Chiefs of Staff Manual (CJCSM), Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND)," March 2005

[7] National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No.1000, "National Information Assurance Certification and Accreditation Process (NIACAP)," April 2000

[8] NCSC-TG-001 "A Guide to Understanding Auditing in Trusted Systems," July 1987

[9] CSC-TG-008 "A Guide to Understanding Configuration Management in Trusted Systems," March 1988

[10] Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems

[11] National Institute of Standards and Technology (NIST) Special Publication 800-37, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems," October 2002

[12] Committee on National Security Systems Security (CNSSI) 4009, "National Information Assurance (IA) Glossary," May 2003

[13] Chief of Naval Operations Information Assurance Publication, Module

5239-13 Vol III "System Security Authorization Agreement (SSAA)" October 2003

[14] Chief of Naval Operations Information Assurance Publication, Module 5239-16 "Risk Assessment Guidebook," March 2003

[15] Gordon Army Base "Required Security Documentation," Retrieved July 2005 from http://ia.gordon.army.mil/iaso/lesson7.htm

[16] Powerpoint Presentation, "Defense Information Assurance Certification and Accreditation Process (DIACAP), DIACAP Knowledge Base and Enterprise Mission Assurance Support System (eMASS)," September 2005

[17] Portillo, A. and Raizada, M. (2004, May 6) "XACTA Web Certification and Evaluation (C&A) Evaluation," Powerpoint Presentation

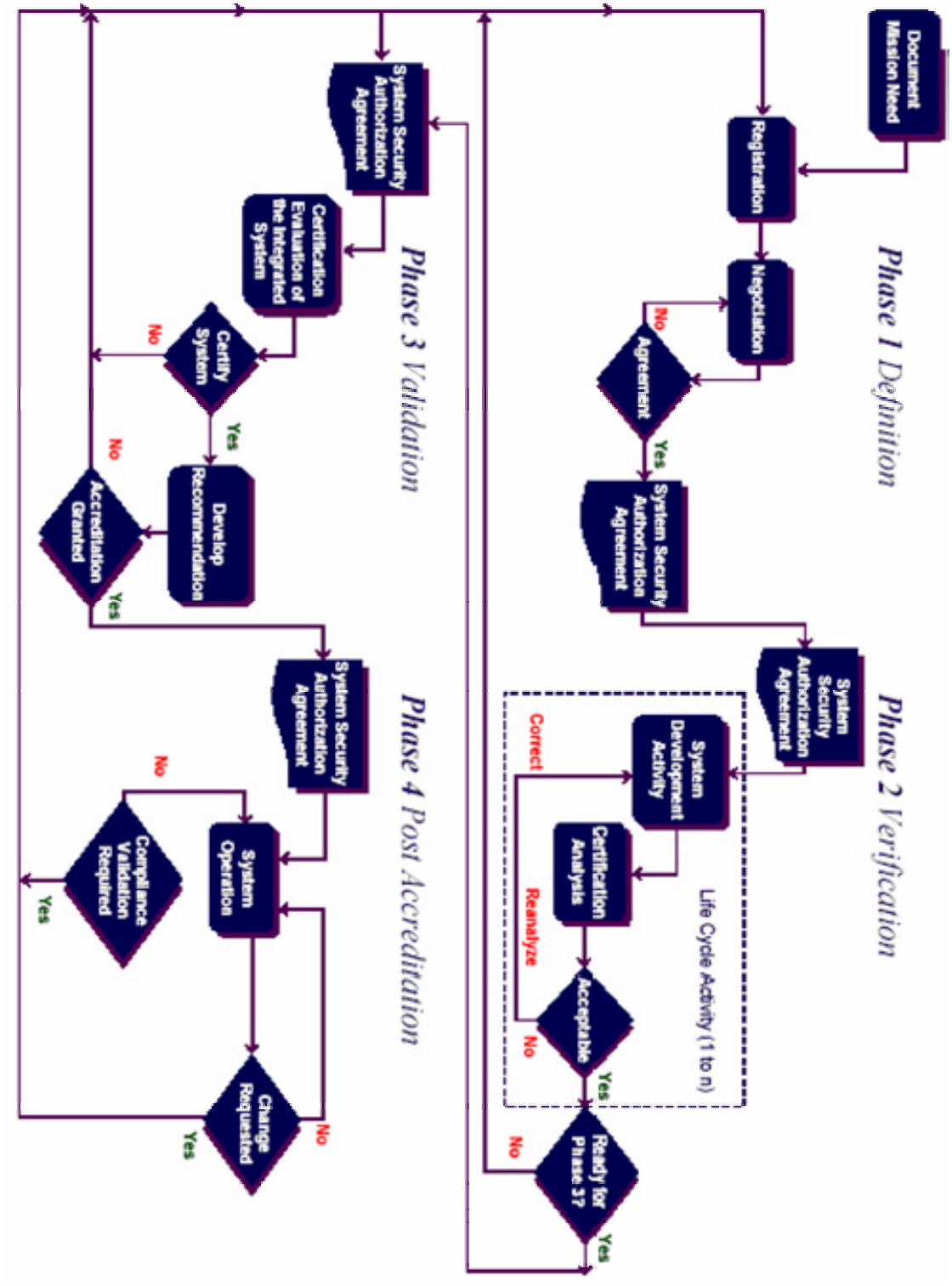
[18] XACTA Information Assurance (IA) Manager (2005, February), "Assessment Engine Getting Started Guide," Retrieved July 2005 from http://www.xacta.com/Solutions/IT%20Security%20Management/Xacta/

[19} Aberdeen Group (2002, November), "Automated Vulnerability Remediation – The Cure for Security's Common Cold," Retrieved September 2005 from http://www.aberdeen.com/2001/research/12023072.asp

[20} Telos Corporation, "XACTA IA Manager Enterprise Edition Build 485, Security Target and Validation Report" Retrieved September 2005 from http://niap.nist.gov/cc-scheme/st/ST_VID3028.html

[21] Military Health System Information Assurance Program Office (2003, December). *Military Health System Information Assurance policy/guidance manual.*

APPENDIX A. FOUR PHASES OF DITSCAP



THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. MESSAGE FROM CNO N64 DTG: 191943Z JUN 00 CERTIFICATION AND ACCREDITATION OF SYSTEMS AND NETWORKS

UNCLASSIFIED
ACTION: BUMED
COG: OLA/ASN FM/ASN MRA/ASN IE/UNSECNAV/DON CIO
R 091943Z JUN 00
FM:CNO WASHINGTON DC//N64//
INFO UNSECNAV WASHINGTON DC//AAUSN//
ASSTSECNAV FM WASHINGTON DC
ASSTSECNAV IE WASHINGTON DC
ASSTSECNAV MRA WASHINGTON DC
CNO WASHINGTON DC//N1/N2/N3/N4/N4T/N43/N5/N6/N7/N8/N82/
N83/N09/
N09B/N095/N096/N097//
OLA WASHINGTON DC

Subject:CERTIFICATION AND ACCREDITATION OF SYSTEMS AND NETWORKS//

UNCLAS //N05239// SECTION 01 OF 02
MSGID/GENADMIN/CNO N64//
SUBJ/CERTIFICATION AND ACCREDITATION OF SYSTEMS AND NETWORKS//

REF/A/DOC/DOD/21MAR88//
REF/B/DOC/DOD/10FEB98//
REF/C/DOC/CNO/09NOV99//
REF/D/DOC/CNO/MAY00//
REF/E/DOC/CNO/MAY00//

NARR/REF A IS DOD DIRECTIVE 5200.28 - SECURITY REQUIREMENTS FOR AUTOMATED
INFORMATION SYSTEMS (AIS'S).
REF B IS DOD INSTRUCTION 5200.40 - DOD INFORMATION SYSTEM TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP).
REF C IS OPNAVINST 5239.1B - NAVY INFORMATION ASSURANCE PROGRAM.
REF D IS DON IA PUB MODULE 5239-01 - INTRODUCTION TO INFORMATION ASSURANCE (IA) GUIDEBOOK.
REF E IS DON IA PUB MODULE 5239-13 - INFORMATION ASSURANCE CERTIFICATION PAGE 06 RUENAAA4545 UNCLAS AND

ACCREDITATION (C&A) PUBLICATION, VOLUMES I - III (DRAFT VOLS I & II ARE POSTED ON THE INFOSEC WEB SITE.
DRAFT VOL III WILL BE POSTED WHEN AVAILABLE).//

POC/MS. LOUISE DAVIDSON/GS-15/N643/CNO/TEL:703-601-1261/DSN:329-1261/EMAIL:DAVIDSON.LOUISE(AT)HQ.NAVY.MIL//
POC/MR. DAVID CROTTY/PMW-161/SPAWAR/TEL:TBD/619-524-7341/DSN:524-7341/EMAIL:CROTTYD(AT)SPAWAR.NAVY.MIL.//

RMKS/1. BACKGROUND. DOD POLICY (REFS A AND B) MANDATES THAT ALL AUTOMATED INFORMATION SYSTEMS (AIS'S),
NETWORKS AND SITES BE CERTIFIED AND ACCREDITED IN ACCORDANCE WITH THE DITSCAP. RECENT NAVY EFFORTS
TO ENFORCE THE NAVY'S FLEET FIREWALL POLICY AND TO COMPLY WITH THE DISN(SIPRNET AND NIPRNET)
CONNECTION APPROVAL PROCESS (CAP) HAVE IDENTIFIED SEVERAL LEGACY AND NEW, NAVY PROGRAM OF RECORD (POR)
DEPLOYABLE AND JOINT/DOD SYSTEMS THAT ARE NOT IN COMPLIANCE WITH THIS POLICY.

2. POLICY AND GUIDANCE. REFS C THRU E PROVIDE SPECIFIC NAVY POLICY AND GUIDANCE IMPLEMENTING REFS A AND B.

IN SUMMARY:
A. ALL DOD SYSTEMS THAT COLLECT, STORE, TRANSMIT OR PROCESS UNCLASSIFIED OR CLASSIFIED INFORMATION
THAT IS ACQUIRED, OPERATED OR SUSTAINED SHALL BE CERTIFIED AND ACCREDITED. THIS INCLUDES
THE PAGE 07RUENAAA4545 UNCLAS DEVELOPMENT OF NEW AIS, THE INCORPORATION OF AIS INTO THEEXISTING
INFRASTRUCTURE, PROTOTYPES, RECONFIGURATIONS OR UPGRADES TO EXISTING SYSTEMS AND LEGACY SYSTEMS.

(1) DESIGNATED APPROVING AUTHORITY (DAA) RESPONSIBILITY FOR NAVY SYSTEMS - A DAA SHALL
BE ASSIGNED FOR EVERY SYSTEM IAW REF C.

(2) SYSTEM SECURITY AUTHORIZATION AGREEMENT (SSAA):

* FOR NAVY INSTALLED FLEET AND LOCALLY ACQUIRED SYSTEMS, PRIOR TO MAKING AN
ACCREDITATION DECISION, DAA'S SHALL ENSURE THAT THE SYSTEMS COMPLY WITH THE MINIMUM
DIRECTION PROVIDED IAW REF E.

* FOR NAVY POR/DEPLOYABLE SYSTEMS, PRIOR TO MAKING AN ACCREDITATION DECISION, DAAS
SHALL ENSURE THAT THE NAVYS CERTIFICATION AUTHORITY (CA - SPAWAR PMW-161) HAS FORMALLY
REVIEWED THE MOST RECENT VERSION OF THE SSAA(GENERATED IAW REF E). UPON REVIEW OF THE SSAA,
THE NAVYS CA SHALL ISSUE A STATEMENT ASSESSING THE QUALITY/ADEQUACY OF THE DOCUMENTED
CERTIFICATION PROCESS AND SPECIFIED SECURITY SOLUTIONS AS WELL AS, WHERE APPROPRIATE,
RECOMMENDATIONS FOR IMPROVING THE SYSTEMS SECURITY POSTURE.

* FOR JOINT/DOD SYSTEMS, THE NAVYS CA SHALL FORMALLY REVIEW THE MOST RECENT VERSION OF
THE SSAA (GENERATED IAW REF B) PRIOR TO INSTALLATION OF ANY NEW SYSTEM OR UPGRADE TO
AN EXISTING SYSTEM AT PAGE 08 RUENAAA4545 UNCLAS ANY NAVY SITE. UPON REVIEW OF THE SSAA,
THE NAVYS CA SHALL ISSUE A STATEMENT ASSESSING THE QUALITY/ADEQUACY OF THE DOCUMENTED
CERTIFICATION PROCESS AND SPECIFIED SECURITY SOLUTIONS AS WELL AS, WHERE APPROPRIATE,
RECOMMENDATIONS FOR IMPROVING THE SYSTEMS SECURITY POSTURE.

* AIS PROCESSING AT MULTIPLE LEVELS OF SECURITY (MLS), BRIDGING MULTIPLE SECURITY LEVELS
(MSL - INCLUDING US-ONLY TO FOREIGN/ALLIED/COALITION CLASSIFIED CONNECTIONS), PERFORMING
COMMUNICATIONS SECURITY(COMSEC), AND/OR SPECIFICALLY DESIGNED TO PROVIDE INFORMATION
SYSTEM SECURITY (INFOSEC), SHALL MEET ADDITIONAL CERTIFICATION REQUIREMENTS AS MANDATED
BY THE SECRET AND BELOW INTEROPERABILITY (SABI) INITIATIVE, NATIONAL SECURITY AGENCY (NSA),
DEFENSE INTELLIGENCE AGENCY (DIA), NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST),
AND/OR NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE (NSTISSC).
CNO N643 OR SPAWAR PMW-161 SHOULD BE CONTACTED FOR SPECIFIC DETAILS.

(3) PRIOR TO INSTALLATION OF ANY NEW POR/DEPLOYABLE SYSTEM, OR UPGRADE/RECONFIGURATION TO
AN EXISTING LEGACY SYSTEM, THE SYSTEM DAA SHALL PROVIDE A FORMAL TYPE ACCREDITATION

DECISION (EITHER INTERIM OR FINAL TYPE APPROVAL TO OPERATE (IATO/ATO) AND A COPY OF THE
SYSTEMS PAGE 09 RUENAAA4545 UNCLAS SSAA TO THE SITE/LOCAL DAA FOR LOCAL IMPLEMENTATION
AND ACCREDITATION.

(4) EXISTING LEGACY SYSTEMS MUST MAINTAIN A CURRENT ACCREDITATION STATUS THROUGHOUT THE
ENTIRE LIFECYCLE OF THE SYSTEM. PROGRAM MANAGERS FOR EXISTING LEGACY SYSTEMS THAT HAVE
NOT BEEN CERTIFIED AND ACCREDITED IN ACCORDANCE WITH THE DITSCAP, OR WHOS DITSCAP BASED
CERTIFICATION AND ACCREDITATION HAS EXPIRED, SHALL EXPEDITIOUSLY TAKE PROACTIVE MEASURES
TO (RE-)CERTIFY AND (RE-)ACCREDIT THE SYSTEM.

B. ALL NAVY NETWORKS SHALL BE CERTIFIED AND ACCREDITED BY THE RESPECTIVE SITE DAA IAW REF C.
PER REF A, THE DAA RESPONSIBLE FOR THE OVERALL SECURITY OF THE NETWORK SHALL HAVE THE AUTHORITY AND
RESPONSIBILITY TO REMOVE FROM THE NETWORK ANY AIS NOT ADHERING TO THE SECURITY REQUIREMENTS OF THE NETWORK.

(1) CERTIFICATION AND ACCREDITATION RESOURCES.

(A) THE NAVY INFOSEC WEB SITE
(HTTP:(SLANT)(SLANT)INFOSEC.NAVY.MIL(SLANT)) POSTS
COPIES OF REFS A THRU F AS WELL AS ADDITIONAL GUIDANCE AND TEMPLATES ASSOCIATED
WITH THE CERTIFICATION AND ACCREDITATION OF SYSTEMS AND NETWORKS. THIS INFORMATION
CAN BE FOUND IN THE INFOSEC SERVICES PORTION OF THE WEB PAGE 10 RUENAAA4545 UNCLAS SITE.

(B) DISA'S INFORMATION ASSURANCE SUPPORT ENVIRONMENT (IASE) WEB SITE (HTTP:(SLANT)(SLANT)MATTCHE.IIIE.DISA.MIL(SLANT))
POSTS COPIES OF REFS A AND B AND ADDITIONAL GUIDANCE,
TEMPLATES, AND TOOLS ASSOCIATED WITH THE CERTIFICATION AND ACCREDITATION OF SYSTEMS.

(C) ALL PROGRAM MANAGERS AND RESPECTIVE RESOURCE SPONSORS ARE RESPONSIBLE FOR PLANNING,
PROGRAMMING AND BUDGETING FOR CERTIFICATION, ACCREDITATION AND ASSOCIATED SECURITY

MEASURES FOR THE AIS THROUGHOUT THE ENTIRE LIFECYCLE OF THE SYSTEM AS DELINEATED IN
THE DITSCAP (REF B).

(D) THE NAVY CERTIFICATION AUTHORITY, SPAWAR PMW-161, SHALL PROVIDE GENERAL PROCEDURAL
AND TECHNICAL ASSISTANCE TO PROGRAMS AND COMMANDS THROUGHOUT THE CERTIFICATION AND
ACCREDITATION PROCESS. PMW-161 IS CURRENTLY RESOURCED TO PROVIDE C&A OVERSIGHT AS
THE NAVY'S CERTIFICATION AUTHORITY. IF REQUIRED, PMW-161 CAN PROVIDE A LIST OF THIRD
PARTY ORGANIZATIONS WHICH CAN SUPPORT PROGRAMS AND COMMANDS WHO DO NOT INHERENTLY
POSSESS THE TECHNICAL AND/OR PROCEDURAL EXPERTISE TO COMPLETE THE ACCREDITATION PROCESS
(FUNDING FOR SUCH SUPPORT SHALL BE THE RESPONSIBILITY OF THE PROGRAM AS DELINEATED
IN SUB-PARA3.C. ABOVE).

AS PART OF A LARGER INFOSEC/IA AWARENESS -ROAD SHOW- FOR
BT
UNCLAS //N05239//
FINAL SECTION OF 02PROGRAM MANAGERS, PMW-161 HAS PREPARED A PRESENTATION TO PROVIDE INFORMATION AND AWARENESS ON
THE DITSCAP BASED CERTIFICATION AND ACCREDITATION PROCESS. COMMANDS DESIRING MORE INFORMATION ON THIS PRESENTATION, ROAD SHOW, OR WITH GENERAL CERTIFICATION AND ACCREDITATION QUESTIONS SHOULD CONTACT PMW-161 DIRECTLY.

4. ACTION. REQUEST ADDEES READDRESS/FORWARD THIS MESSAGE, AS APPROPRIATE, TO COMMANDS/PROGRAMS WITHIN THEIR CLAIMANCY/AREA OF RESPONSIBILITY.//

BT
#4545

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Karen Burke
   Department of Information Sciences, Code CS
   Naval Postgraduate School
   Monterey, California

4. Douglas Brinkley
   Department of Information Sciences, Code IS
   Naval Postgraduate School
   Monterey, California

5. Dan C. Boger
   Department of Information Sciences, Code IS
   Naval Postgraduate School
   Monterey, California